

ORAL ARGUMENT NOT YET SCHEDULED

No. 17-5171

**IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT**

ELECTRONIC PRIVACY INFORMATION CENTER

Plaintiff-Appellant,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et
al.,*

Defendants-Appellees.

**On Appeal from an Order of the
U.S. District Court for the District of Columbia
Case No. 17-cv-1320(CKK)**

JOINT APPENDIX

MARK B. STERN
DANIEL TENNY
*Attorneys, Appellate Staff
Civil Division*
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
(202) 514-1838
Counsel for Defendants-Appellees

MARC ROTENBERG
ALAN BUTLER
CAITRIONA FITZGERALD
JERAMIE SCOTT
JOHN DAVISSON
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff-Appellant

INDEX TO JOINT APPENDIX

	Page
District Court Docket Sheet	JA 000001
Memorandum Opinion (ECF No. 40).....	JA 000014
Order (ECF No. 41)	JA 000049
Declaration of Kris W. Kobach, (July 5, 2017) (ECF No. 8-1).....	JA 000050
Exec. Order. No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017) (ECF No. 8-1 Ex. 1)	JA 000054
Charter, Presidential Advisory Commission on Election Integrity (June 23, 2017) (ECF No. 8-1 Ex. 2)	JA 000057
Letter from Kris Kobach, Vice Chair, Presidential Advisory Commission on Election Integrity, to John Merrill, Secretary of State, Alabama (June 28, 2017) (ECF No. 8-1 Ex. 3).....	JA 000060
Second Declaration of Kris W. Kobach, (July 6, 2017) (ECF No. 11-1)	JA 000063
Transcript of Temporary Restraining Order (July 7, 2017) (ECF No. 22)	JA 000066
Third Declaration of Kris W. Kobach, (July 10, 2017) (ECF No. 24-1)	JA 000129
E-mail from Andrew Kossack, Designated Federal Officer, Presidential Advisory Commission on Election Integrity to state election officials (July 10, 2017, 09:40 AM ET) (ECF No. 24-1 Ex. A)	JA 000131
Second Amended Complaint (July 11, 2017) (ECF No. 33)	JA 000132

Exhibits to Plaintiff's Amended Motion (ECF No. 35):

Memorandum M-03-22 from Josh Bolten, Dir. of Office of Mgmt. & Budget, to Heads of Exec. Dep'ts & Agencies (Sep. 23, 2003).....	JA 000148
<i>Perkins v. Dep't of Veteran Affairs</i> , No. 07-310 (N.D. Ala. Apr. 21, 2010).....	JA 000161
Presentation by Kris W. Kobach to the National Ass'n of State Election Dirs., Interstate Voter Registration Crosscheck Program (Jan. 26, 2013).....	JA 000185
Sec'y of State, Kansas, Interstate Crosscheck Program Grows (2013).....	JA 000201
Privacy Impact Assessment (PIA) for the Safe Access File Exchange ("SAFE"), Dep't of Defense (2015).....	JA 000209
Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology, 2015 Daily Comp. Pres. Doc. 185 (March 19, 2015).....	JA 000215
Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017).....	JA 000219
Letter from Kris Kobach, Vice Chair, Presidential Advisory Commission on Election Integrity, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017).....	JA 000221
Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Website (July 3, 2017 12:02 AM).....	JA 000223
Letter from Electronic Privacy Information Center (EPIC), to National Association of State Secretaries (July 3, 2017).....	JA 000224

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).....	JA 000228
Declaration of Marc Rotenberg (July 7, 2017).....	JA 000229
Webpage: Privacy Impact Assessments (PIA), U.S. General Services Administration, (July 7, 2017).....	JA 000231
Declaration of Charles Christopher Herndon, (July 17, 2017) (ECF No. 38-1).....	JA 000233
Declaration of Eleni Kyriakides, (July 17, 2017) (ECF No. 39-1).....	JA 000236

APPEAL,TYPE-D

**U.S. District Court
District of Columbia (Washington, DC)
CIVIL DOCKET FOR CASE #: 1:17-cv-01320-CKK**

ELECTRONIC PRIVACY INFORMATION CENTER v.
PRESIDENTIAL ADVISORY COMMISSION ON ELECTION
INTEGRITY et al

Assigned to: Judge Colleen Kollar-Kotelly

Cases: [1:17-cv-01351-CKK](#)
[1:17-cv-01354-CKK](#)

Case in other court: USCA, 17-05171

Cause: 05:702 Administrative Procedure Act

Date Filed: 07/03/2017

Jury Demand: None

Nature of Suit: 899 Administrative
Procedure Act/Review or Appeal of
Agency Decision

Jurisdiction: U.S. Government Defendant

Plaintiff

**ELECTRONIC PRIVACY
INFORMATION CENTER**

represented by **Marc Rotenberg**
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140, ext 106
Fax: (202) 483-1248
Email: rotenberg@epic.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Alan Jay Butler
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140 ext 103
Fax: (202) 483-1248
Email: butler@epic.org
ATTORNEY TO BE NOTICED

Caitriona Fitzgerald
ELECTRONIC PRIVACY
INFORMATION CENTER
14 Tyler Street
Third Floor
Somerville, MA 02143

(617) 94508409
PRO HAC VICE
ATTORNEY TO BE NOTICED

Jeramie D. Scott
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140
Fax: (202) 483-1248
Email: jscott@epic.org
ATTORNEY TO BE NOTICED

V.

Defendant

**PRESIDENTIAL ADVISORY
COMMISSION ON ELECTION
INTEGRITY**

represented by **Carol Federighi**
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514-1903
Email: carol.federighi@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514-5302
Fax: (202) 616-8202
Email: Elizabeth.Shapiro@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
U.S. DEPARTMENT OF JUSTICE
P.O. Box 883
Washington, DC 20044
(202) 514-1944
Fax: (202) 616-8460
Email: joseph.borson@usdoj.gov
LEAD ATTORNEY

ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
US DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Suite 7000
Washington, DC 20001
(202) 353-4519
Email: kristina.wolfe@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

MICHAEL PENCE

*In his official capacity as Chair of the
Presidential Advisory Commission on
Election Integrity*

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

KRIS KOBACH

*In his official capacity as Vice Chair of the
Presidential Advisory Commission on
Election Integrity*

represented by **Carol Federighi**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)

*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Kristina Ann Wolfe
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Defendant

**EXECUTIVE OFFICE OF THE
PRESIDENT OF THE UNITED
STATES**

represented by **Carol Federighi**
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Elizabeth J. Shapiro
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Joseph Evan Borson
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Kristina Ann Wolfe
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Defendant

**OFFICE OF THE VICE PRESIDENT
OF THE UNITED STATES**

represented by **Carol Federighi**
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Elizabeth J. Shapiro
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Joseph Evan Borson
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Kristina Ann Wolfe
(See above for address)

*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Defendant

**GENERAL SERVICES
ADMINISTRATION**

represented by **Carol Federighi**
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Elizabeth J. Shapiro
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Joseph Evan Borson
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Kristina Ann Wolfe
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Defendant

U.S. DEPARTMENT OF DEFENSE

represented by **Carol Federighi**
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Kristina Ann Wolfe
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Defendant

CHARLES G. HERNDON
*in his official capacity as Director of White
House Information Technology*

represented by **Joseph Evan Borson**
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Kristina Ann Wolfe
(See above for address)
*LEAD ATTORNEY
ATTORNEY TO BE NOTICED*

Defendant

UNITED STATES DIGITAL SERVICE

represented by **Kristina Ann Wolfe**
 (See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant**EXECUTIVE COMMITTEE FOR
PRESIDENTIAL INFORMATION
TECHNOLOGY**

represented by **Joseph Evan Borson**
 (See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Kristina Ann Wolfe
 (See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
07/03/2017	1	COMPLAINT against EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Filing fee \$ 400, receipt number 4616085803) filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Civil Cover Sheet)(td) (Entered: 07/03/2017)
07/03/2017		SUMMONS (8) Issued as to EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, U.S. Attorney and U.S. Attorney General (td) (Entered: 07/03/2017)
07/03/2017	2	LCvR 7.1 CERTIFICATE OF DISCLOSURE of Corporate Affiliations and Financial Interests by ELECTRONIC PRIVACY INFORMATION CENTER (td) (Entered: 07/03/2017)
07/03/2017	3	MOTION for Temporary Restraining Order by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Exhibit, # 2 Text of Proposed Order)(td) (Entered: 07/03/2017)
07/03/2017		MINUTE ORDER: At approximately 4:50 P.M. EST, the Court held an on-the-record teleconference, attended by counsel for both parties, to set a briefing schedule on Plaintiff's 3 Emergency Motion for a Temporary Restraining Order. Defendants shall file their opposition to the motion by 4 P.M. EST on WEDNESDAY, JULY 5, 2017. Plaintiff shall file its reply by 9 A.M. EST on THURSDAY, JULY 6, 2017. Signed by Judge Colleen Kollar-Kotelly on 7/3/2017. (lcckk1) (Entered: 07/03/2017)
07/03/2017	4	ORDER Establishing Procedures for Cases Assigned to Judge Colleen Kollar-Kotelly.

		Signed by Judge Colleen Kollar-Kotelly on 07/03/2017. (DM) (Entered: 07/03/2017)
07/03/2017	5	NOTICE of Appearance by Elizabeth J. Shapiro on behalf of All Defendants (Shapiro, Elizabeth) (Entered: 07/03/2017)
07/03/2017		Minute Entry for proceedings held before Judge Colleen Kollar-Kotelly: Telephone Conference held on 7/3/2017. (Court Reporter Richard Ehrlich.) (dot) (Entered: 07/07/2017)
07/05/2017	6	NOTICE of Appearance by Carol Federighi on behalf of All Defendants (Federighi, Carol) (Entered: 07/05/2017)
07/05/2017	7	NOTICE of Appearance by Joseph Evan Borson on behalf of EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Borson, Joseph) (Entered: 07/05/2017)
07/05/2017	8	RESPONSE re 3 MOTION for Temporary Restraining Order filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration of Kris Kobach, # 2 Text of Proposed Order)(Federighi, Carol) (Entered: 07/05/2017)
07/05/2017	9	ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/5/2017. (lcckk1) (Entered: 07/05/2017)
07/06/2017	10	<p>TRANSCRIPT OF SCHEDULING CONFERENCE before Judge Colleen Kollar-Kotelly held on July 3, 2017; Page Numbers: 1- 13. Date of Issuance: July 6, 2017. Court Reporter/Transcriber Richard D. Ehrlich, Telephone number 202-354-3269, Transcripts may be ordered by submitting the Transcript Order Form</p> <p>For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi-page, condensed, CD or ASCII) may be purchased from the court reporter.</p> <p>NOTICE RE REDACTION OF TRANSCRIPTS: The parties have twenty-one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov.</p> <p>Redaction Request due 7/27/2017. Redacted Transcript Deadline set for 8/6/2017. Release of Transcript Restriction set for 10/4/2017.(Ehrlich, Richard) Modified date of hearing on 7/7/2017 (znmw). (Entered: 07/06/2017)</p>
07/06/2017	11	RESPONSE TO ORDER OF THE COURT re 9 Order filed by EXECUTIVE OFFICE

		OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration of Kris W. Kobach)(Borson, Joseph) (Entered: 07/06/2017)
07/06/2017	12	NOTICE of Appearance by Alan Jay Butler on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (Butler, Alan) (Entered: 07/06/2017)
07/06/2017	13	REPLY to opposition to motion re 3 MOTION for Temporary Restraining Order filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Addendum, # 2 Affirmation of Marc Rotenberg, # 3 Exhibits 1-11)(Butler, Alan) (Entered: 07/06/2017)
07/06/2017	14	ERRATA by ELECTRONIC PRIVACY INFORMATION CENTER 13 Reply to opposition to Motion filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Corrected Exhibit 11)(Butler, Alan) (Entered: 07/06/2017)
07/06/2017	15	ORDER. The Court hereby sets a hearing on Plaintiff's 3 Motion for a Temporary Restraining Order, to be held at 4:00 P.M. on July 7, 2017, in Courtroom 28A. Signed by Judge Colleen Kollar-Kotelly on 7/6/2017. (lcckk1) (Entered: 07/06/2017)
07/06/2017		Set/Reset Hearings: Motion Hearing set for 7/7/2017 at 4:00 PM in Courtroom 28A before Judge Colleen Kollar-Kotelly. (dot) (Entered: 07/07/2017)
07/07/2017	16	Unopposed MOTION for Leave to File <i>Surreply</i> by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY (Attachments: # 1 Exhibit Proposed Surreply, # 2 Text of Proposed Order)(Federighi, Carol) (Entered: 07/07/2017)
07/07/2017	17	RESPONSE TO ORDER OF THE COURT <i>Filing of Supplemental Brief</i> by ELECTRONIC PRIVACY INFORMATION CENTER re 15 Order (Butler, Alan) Modified event title on 7/10/2017 (znmw). (Entered: 07/07/2017)
07/07/2017	18	RESPONSE TO ORDER OF THE COURT re 15 Order <i>Defendants' Supplemental Brief on Informational Standing</i> filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Borson, Joseph) (Entered: 07/07/2017)
07/07/2017	19	Unopposed MOTION for Leave to File <i>Sur-surreply</i> by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Exhibit Proposed sur-surreply, # 2 Exhibit Exhibit to proposed sur-surreply, # 3 Text of Proposed Order)(Butler, Alan) (Entered: 07/07/2017)
07/07/2017	20	NOTICE of <i>Supplemental Exhibits</i> by ELECTRONIC PRIVACY INFORMATION CENTER re 15 Order (Attachments: # 1 Supplemental Exhibits)(Butler, Alan) (Entered: 07/07/2017)

07/07/2017		Minute Entry for proceedings held before Judge Colleen Kollar-Kotelly: Motion Hearing held on 7/7/2017 re 3 MOTION for Temporary Restraining Order filed by ELECTRONIC PRIVACY INFORMATION CENTER; and taken under advisement. (Court Reporter Richard Ehrlich.) (dot) (Entered: 07/07/2017)
07/07/2017	21	AMENDED COMPLAINT <i>pursuant to FRCP 15(a)(1)(A)</i> against ELECTRONIC PRIVACY INFORMATION CENTER filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Summons as to U.S. Department of Defense)(Butler, Alan) (Entered: 07/07/2017)
07/09/2017	22	<p>TRANSCRIPT OF TEMPORARY RESTRAINING ORDER before Judge Colleen Kollar-Kotelly held on July 7, 2017; Page Numbers: 1 - 63. Date of Issuance: July 10, 2017. Court Reporter/Transcriber Richard D. Ehrlich, Telephone number (202) 354-3269, Transcripts may be ordered by submitting the Transcript Order Form</p> <p>For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi-page, condensed, CD or ASCII) may be purchased from the court reporter.</p> <p>NOTICE RE REDACTION OF TRANSCRIPTS: The parties have twenty-one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov.</p> <p>Redaction Request due 7/30/2017. Redacted Transcript Deadline set for 8/9/2017. Release of Transcript Restriction set for 10/7/2017.(Ehrlich, Richard) (Entered: 07/09/2017)</p>
07/10/2017	23	ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/10/2017. (lcckk1) (Entered: 07/10/2017)
07/10/2017		Set/Reset Deadline: Supplemental briefing due by 4:00 PM on 7/10/2017. (tth) (Entered: 07/10/2017)
07/10/2017	24	RESPONSE TO ORDER OF THE COURT re 23 Order <i>Supplemental Brief re: DOD</i> filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY. (Attachments: # 1 Declaration Third Kobach Decl.)(Borson, Joseph) (Entered: 07/10/2017)
07/10/2017	25	SUMMONS (1) Issued Electronically as to U.S. DEPARTMENT OF DEFENSE. (znmw) (Entered: 07/10/2017)
07/10/2017	26	ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/10/2017. (lcckk1) (Entered: 07/10/2017)

		07/10/2017)
07/11/2017	27	RESPONSE TO ORDER OF THE COURT re 26 Order filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Butler, Alan) (Entered: 07/11/2017)
07/11/2017	28	NOTICE of Appearance by Jeramie D. Scott on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (Scott, Jeramie) (Entered: 07/11/2017)
07/11/2017	29	MOTION for Leave to Appear Pro Hac Vice :Attorney Name- Caitriona Fitzgerald, :Firm- Electronic Privacy Information Center, :Address- 14 Tyler Street, Third Floor, Somerville, MA 02143. Phone No. - (617) 945-8409. Filing fee \$ 100, receipt number 0090-5026343. Fee Status: Fee Paid. by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Declaration of Caitriona Fitzgerald, # 2 Text of Proposed Order)(Rotenberg, Marc) (Entered: 07/11/2017)
07/11/2017	30	MOTION for Leave to File <i>a Second Amended Complaint</i> by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1 Second Amended Complaint, # 2 Exhibit 5, # 3 Summons as to Charles C. Herndon, # 4 Summons as to U.S. Digital Service, # 5 Summons as to Executive Committee for Presidential Information Technology, # 6 Text of Proposed Order)(Butler, Alan) (Entered: 07/11/2017)
07/11/2017	31	ORDER. Signed by Judge Colleen Kollar-Kotelly on 7/11/2017. (lcckk1) (Entered: 07/11/2017)
07/11/2017	32	RESPONSE re 30 MOTION for Leave to File <i>a Second Amended Complaint</i> filed by EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, U.S. DEPARTMENT OF DEFENSE. (Federighi, Carol) (Entered: 07/11/2017)
07/11/2017		MINUTE ORDER: For good cause shown, and in light of Defendants' notice that they do not oppose this relief, ECF No. 32, Plaintiff's 30 Motion for Leave to File a Second Amended Complaint is GRANTED. Signed by Judge Colleen Kollar-Kotelly on 7/11/2017. (lcckk1) (Entered: 07/11/2017)
07/11/2017	33	SECOND AMENDED COMPLAINT against GENERAL SERVICES ADMINISTRATION, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE, PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, U.S. DEPARTMENT OF DEFENSE, CHARLES G. HERNDON, UNITED STATES DIGITAL SERVICE, EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Exhibit 5) (znmw) (Entered: 07/12/2017)
07/12/2017	34	SUMMONS (3) Issued Electronically as to EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY, CHARLES G. HERNDON, UNITED STATES DIGITAL SERVICE. (znmw) (Entered: 07/12/2017)
07/13/2017	35	Amended MOTION for Temporary Restraining Order , MOTION for Preliminary Injunction by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # 1

		Memorandum in Support, # 2 Exhibit List, # 3 Exhibit 1-20, # 4 Exhibit 21-30, # 5 Exhibit 31-40, # 6 Text of Proposed Order)(Butler, Alan) (Entered: 07/13/2017)
07/13/2017	36	ERRATA <i>Corrected Exhibits 21-30</i> by ELECTRONIC PRIVACY INFORMATION CENTER 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Exhibit 21-30)(Butler, Alan) (Entered: 07/13/2017)
07/16/2017	37	NOTICE of Appearance by Kristina Ann Wolfe on behalf of All Defendants (Wolfe, Kristina) (Entered: 07/16/2017)
07/17/2017	38	RESPONSE re 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY, EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES, GENERAL SERVICES ADMINISTRATION, CHARLES G. HERNDON, KRIS KOBACH, OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES, MICHAEL PENCE. (Attachments: # 1 Declaration, # 2 Text of Proposed Order)(Borson, Joseph) (Entered: 07/17/2017)
07/17/2017	39	REPLY to opposition to motion re 35 Amended MOTION for Temporary Restraining Order MOTION for Preliminary Injunction filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Declaration of Eleni Kyriakides)(Butler, Alan) (Entered: 07/17/2017)
07/18/2017		NOTICE OF ERROR re 39 Reply to opposition to Motion; emailed to butler@epic.org, cc'd 9 associated attorneys -- The PDF file you docketed contained errors: 1. FYI on future filings, the signature of the person filing and the one signing the document must match. (ztd,) (Entered: 07/18/2017)
07/24/2017	40	MEMORANDUM OPINION. Signed by Judge Colleen Kollar-Kotelly on 7/24/2017. (lcckk1) (Entered: 07/24/2017)
07/24/2017	41	ORDER. Plaintiff's 35 Motion for a Temporary Restraining Order and Preliminary Injunction is DENIED WITHOUT PREJUDICE. Signed by Judge Colleen Kollar-Kotelly on 7/24/2017. (lcckk1) (Entered: 07/24/2017)
07/25/2017	42	NOTICE OF APPEAL TO DC CIRCUIT COURT as to 41 Order on Motion for TRO, Order on Motion for Preliminary Injunction by ELECTRONIC PRIVACY INFORMATION CENTER. Filing fee \$ 505, receipt number 0090-5047166. Fee Status: Fee Paid. Parties have been notified. (Attachments: # 1 Exhibit 1)(Rotenberg, Marc) (Entered: 07/25/2017)
07/26/2017	43	Transmission of the Notice of Appeal, Order Appealed (Memorandum Opinion), and Docket Sheet to US Court of Appeals. The Court of Appeals fee was paid this date re 42 Notice of Appeal to DC Circuit Court. (znmw) (Entered: 07/26/2017)
07/27/2017		USCA Case Number 17-5171 for 42 Notice of Appeal to DC Circuit Court, filed by ELECTRONIC PRIVACY INFORMATION CENTER. (zrdj) (Entered: 07/27/2017)
08/02/2017	44	RETURN OF SERVICE/AFFIDAVIT of Summons and Complaint Executed as to the United States Attorney. Date of Service Upon United States Attorney on 7/16/2017.

		Answer due for ALL FEDERAL DEFENDANTS by 9/4/2017. (Rotenberg, Marc) Modified dates on 8/3/2017 (znmw). (Entered: 08/02/2017)
08/02/2017	45	RETURN OF SERVICE/AFFIDAVIT of Summons and Complaint Executed on United States Attorney General. Date of Service Upon United States Attorney General 7/6/2017. (Rotenberg, Marc) Modified date of service on 8/3/2017 (znmw). (Entered: 08/02/2017)
08/02/2017	46	RETURN OF SERVICE/AFFIDAVIT of Summons and Complaint Executed. EXECUTIVE COMMITTEE FOR PRESIDENTIAL INFORMATION TECHNOLOGY served on 7/24/2017; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES served on 7/6/2017; GENERAL SERVICES ADMINISTRATION served on 7/6/2017; CHARLES G. HERNDON served on 7/24/2017; KRIS KOBACH served on 7/6/2017; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES served on 7/6/2017; MICHAEL PENCE served on 7/6/2017; PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY served on 7/6/2017; U.S. DEPARTMENT OF DEFENSE served on 7/24/2017; UNITED STATES DIGITAL SERVICE served on 7/24/2017 (Rotenberg, Marc) (Entered: 08/02/2017)
08/11/2017		<p>MINUTE ORDER: The 3 Motion for Temporary Restraining Order and related 16 Motion for Leave to File Surreply, and 17 Motion for Leave to File Sur-surreply, are DENIED AS MOOT. The Court previously ordered Plaintiff to file an amended motion for injunctive relief. Order, ECF No. 31. The 35 Amended Motion for Temporary Restraining Order and Preliminary Injunction was resolved by the Court's July 24, 2017 Memorandum Opinion, ECF No. 40.</p> <p>Separately, the Court has received the 29 Motion for Admission Pro Hac Vice of attorney Caitriona Fitzgerald. That Motion is GRANTED CONTINGENT on Ms. Fitzgerald filing a declaration, by AUGUST 18, 2017, certifying to the Court that she is familiar with the Local Rules of this Court.</p> <p>(lcckk1) (Entered: 08/11/2017)</p>
08/16/2017	47	RESPONSE TO ORDER OF THE COURT re Order on Motion for Leave to Appear Pro Hac Vice,,,, Order on Motion for TRO,,,, Order on Motion for Leave to File,,,,,, filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # 1 Declaration of Caitriona Fitzgerald)(Butler, Alan) (Entered: 08/16/2017)

PACER Service Center			
Transaction Receipt			
08/17/2017 21:15:12			
PACER Login:	ep0116:2545265:0	Client Code:	
Description:	Docket Report	Search Criteria:	1:17-cv-01320-CKK

Billable Pages:	10	Cost:	1.00
------------------------	----	--------------	------

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

ELECTRONIC PRIVACY
INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY
COMMISSION ON ELECTION
INTEGRITY, *et al.*,

Defendants.

Civil Action No. 17-1320 (CKK)

MEMORANDUM OPINION

(July 24, 2017)

This case arises from the establishment by Executive Order of the Presidential Advisory Commission on Election Integrity (the “Commission”), and a request by that Commission for each of the 50 states and the District of Columbia to provide it with certain publicly available voter roll information. Pending before the Court is Plaintiff’s [35] Amended Motion for Temporary Restraining Order and Preliminary Injunction, which seeks injunctive relief prohibiting Defendants from “collecting voter roll data from states and state election officials” and directing Defendants to “delete and disgorge any voter roll data already collected or hereafter received.” Proposed TRO, ECF No. 35-6, at 1-2.

Although substantial public attention has been focused on the Commission’s request, the legal issues involved are highly technical. In addition to the Fifth Amendment of the Constitution, three federal laws are implicated: the Administrative Procedure Act, 5 U.S.C. § 551 *et seq.* (“APA”), the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (“E-Government Act”), and the Federal Advisory Committee Act, codified at 5 U.S.C. app. 2 (“FACA”). All three are likely unfamiliar to the vast majority of Americans, and even seasoned legal practitioners are unlikely to have encountered the latter two.

Matters are further complicated by the doctrine of standing, a Constitutional prerequisite for this Court to consider the merits of this lawsuit.

Given the preliminary and emergency nature of the relief sought, the Court need not at this time decide conclusively whether Plaintiff is, or is not, ultimately entitled to relief on the merits. Rather, if Plaintiff has standing to bring this lawsuit, then relief may be granted if the Court finds that Plaintiff has a likelihood of succeeding on the merits, that it would suffer irreparable harm absent injunctive relief, and that other equitable factors—that is, questions of fairness, justice, and the public interest—warrant such relief.

The Court held a lengthy hearing on July 7, 2017, and has carefully reviewed the parties' voluminous submissions to the Court, the applicable law, and the record as a whole. Following the hearing, additional defendants were added to this lawsuit, and Plaintiff filed the pending, amended motion for injunctive relief, which has now been fully briefed. For the reasons detailed below, the Court finds that Plaintiff has standing to seek redress for the informational injuries that it has allegedly suffered as a result of Defendants declining to conduct and publish a Privacy Impact Assessment pursuant to the E-Government Act prior to initiating their collection of voter roll information. Plaintiff does not, however, have standing to pursue Constitutional or statutory claims on behalf of its advisory board members.

Although Plaintiff has won the standing battle, it proves to be a Pyrrhic victory. The E-Government Act does not itself provide for a cause of action, and consequently, Plaintiff must seek judicial review pursuant to the APA. However, the APA only applies to “agency action.” Given the factual circumstances presently before the Court—which have changed substantially since this case was filed three weeks ago—Defendants' collection of voter

roll information does not currently involve agency action. Under the binding precedent of this circuit, entities in close proximity to the President, which do not wield “substantial independent authority,” are not “agencies” for purposes of the APA. On this basis, neither the Commission or the Director of White House Information Technology—who is currently charged with collecting voter roll information on behalf of the Commission—are “agencies” for purposes of the APA, meaning the Court cannot presently exert judicial review over the collection process. To the extent the factual circumstances change, however—for example, if the *de jure* or *de facto* powers of the Commission expand beyond those of a purely advisory body—this determination may need to be revisited. Finally, the Court also finds that Plaintiff has not demonstrated an irreparable informational injury—given that the law does not presently entitle it to information—and that the equitable and public interest factors are in equipoise. These interests may very well be served by additional disclosure, but they would not be served by this Court, without a legal mandate, ordering the disclosure of information where no right to such information currently exists. Accordingly, upon consideration of the pleadings,¹ the relevant legal authorities, and the record as a whole, Plaintiff’s [35] Motion for a Temporary Restraining Order and Preliminary Injunction is **DENIED WITHOUT PREJUDICE**.²

¹ The Court’s consideration has focused on the following documents:

- Mem. in Supp. of Pl.’s Am. Mot. for a TRO and Prelim. Inj., ECF No. 35-1 (“Pls. Am. Mem.”);
- Defs.’ Mem. in Opp’n to Pl.’s Am. Mot. for a TRO and Prelim. Inj., ECF No. 38 (“Am. Opp’n Mem.”);
- Reply in Supp. of Pl.’s Am. Mot. for a TRO and Prelim. Inj., ECF No. 39 (“Am. Reply Mem.”).

² For the avoidance of doubt, the Court denies without prejudice both Plaintiff’s motion for a temporary restraining order, and its motion for a preliminary injunction.

I. BACKGROUND

The Commission was established by Executive Order on May 11, 2017. Executive Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017) (“Exec. Order”). According to the Executive Order, the Commission’s purpose is to “study the registration and voting processes used in Federal elections.” *Id.* § 3. The Executive Order states that the Commission is “solely advisory,” and that it shall disband 30 days after submitting a report to the President on three areas related to “voting processes” in federal elections. *Id.* §§ 3, 6. The Vice President is the chair of the Commission, and the President may appoint 15 additional members. From this group, the Vice President is permitted to appoint a Vice Chair of the Commission. The Vice President has named Kris W. Kobach, Secretary of State for Kansas, to serve as the Vice Chair. Decl. of Kris Kobach, ECF No. 8-1 (“Kobach Decl.”), ¶ 1. Apart from the Vice President and the Vice Chair, there are presently ten other members of the Commission, including Commissioner Christy McCormick of the Election Assistance Commission (the “EAC”), who is currently the only federal agency official serving on the Commission, and a number of state election officials, both Democratic and Republican, and a Senior Legal Fellow of the Heritage Foundation. *Lawyers’ Committee for Civil Rights Under the Law v. Presidential Advisory Commission on Election Integrity*, No. 17-cv-1354 (D.D.C. July 10, 2017), Decl. of Andrew J. Kossack, ECF No. 15-1 (“Kossack Decl.”), ¶ 1; Second Decl. of Kris W. Kobach, ECF No. 11-1 (“Second Kobach Decl.”), ¶ 1. According to Defendants, “McCormick is not serving in her official capacity as a member of the EAC.” Second Kobach Decl. ¶ 2. The Executive Order also provides that the General Services Administration (“GSA”), a federal agency, will “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,” and that other federal agencies “shall endeavor to cooperate with the Commission.” Exec. Order, § 7.

Following his appointment as Vice Chair, Mr. Kobach directed that identical letters “be sent to the secretaries of state or chief election officers of each of the fifty states and the District of Columbia.” Kobach Decl. ¶ 4. In addition to soliciting the views of state officials on certain election matters by way of seven broad policy questions, each of the letters requests that state officials provide the Commission with the “publicly available voter roll data” of their respective states, “including, if publicly available under the laws of [their] state, the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.” Kobach Decl., Ex. 3 (June 28, 2017 Letter to the Honorable John Merrill, Secretary of State of Alabama). The letters sent by Mr. Kobach also indicate that “[a]ny documents that are submitted to the full Commission will . . . be made available to the public.” *Id.* Defendants have represented that this statement applies only to “narrative responses” submitted by states to the Commission. *Id.* ¶ 5. “With respect to voter roll data, the Commission intends to de-identify any such data prior to any public release of documents. In other words, the voter rolls themselves will not be released to the public by the Commission.” *Id.* The exact process by which de-identification and publication of voter roll data will occur has yet to be determined. Hr’g Tr. 36:20–37:8.

Each letter states that responses may be submitted electronically to an email address, ElectionIntegrityStaff@ovp.eop.gov, “or by utilizing the Safe Access File Exchange (‘SAFE’), which is a secure FTP site the federal government uses for transferring large data files.” Kobach Decl., Ex. 3. The SAFE website is accessible at <https://safe.amrdec.army.mil/safe/Welcome.aspx>. Defendants have represented that it was their intention that “narrative responses” to the letters’ broad policy questions should be sent via email, while voter roll information should be uploaded by using the SAFE system. *Id.* ¶ 5.

According to Defendants, the email address named in the letters “is a White House email address (in the Office of the Vice President) and subject to the security protecting all White House communications and networks.” *Id.* Defendants, citing security concerns, declined to detail the extent to which other federal agencies are involved in the maintenance of the White House computer system. Hr’g Tr. 35:2-10. The SAFE system, however, is operated by the U.S. Army Aviation and Missile Research Development and Engineering Center, a component of the Department of Defense. Second Kobach Decl. ¶ 4; Hr’g Tr. 32:6-9. The SAFE system was “originally designed to provide Army Missile and Research, Development and Engineering Command (AMRDEC) employees and those doing business with AMRDEC an alternate way to send files.” Safe Access File Exchange (Aug. 8, 2012), *available at* <http://www.doncio.navy.mil/ContentView.aspx?id=4098> (last accessed July 20, 2017). The system allows “users to send up to 25 files securely to recipients within the .mil or .gov domains[,]” and may be used by anyone so long as the recipient has a .mil or .gov email address. After an individual uploads data via the SAFE system, the intended recipient receives an email message indicating that “they have been

given access to a file” on the system, and the message provides instructions for accessing the file. The message also indicates the date on which the file will be deleted. This “deletion date” is set by the originator of the file, and the default deletion date is seven days after the upload date, although a maximum of two weeks is permitted.

Defendants portrayed the SAFE system as a conduit for information. Once a state had uploaded voter roll information via the system, Defendants intended to download the data and store it on a White House computer system. Second Kobach Decl. ¶ 5. The exact details of how that would happen, and who would be involved, were unresolved at the time of the hearing. Hr’g Tr. 34:3–35:10; 35:23–36:9. Nonetheless, there is truth to Defendants’ description. Files uploaded onto the system are not archived after their deletion date, and the system is meant to facilitate the transfer of files from one user to another, and is not intended for long-term data storage. As Defendants conceded, however, files uploaded onto the SAFE system are maintained for as many as fourteen days on a computer system operated by the Department of Defense. Hr’g Tr. 31:7–32:5; 36:1–9 (The Court: “You seem to be indicating that DOD’s website would maintain it at least for the period of time until it got transferred, right?” Ms. Shapiro: “Yes. This conduit system would have it for – until it’s downloaded. So from the time it’s uploaded until the time it’s downloaded for a maximum of two weeks and shorter if that’s what’s set by the states.”). Defendants stated that as of July 7, only the state of Arkansas had transmitted voter roll information to the Commission by uploading it to the SAFE system. Hr’g Tr. 40:10–18. According to Defendants, the Commission had not yet downloaded Arkansas’ voter data; and as of the date of the hearing, the data continued to reside on the SAFE system. *Id.*

Shortly after the hearing, Plaintiff amended its complaint pursuant to Federal Rule

of Civil Procedure 15(a)(1)(A), and added the Department of Defense as a defendant. Am. Compl., ECF No. 21. The Court then permitted Defendants to file supplemental briefing with respect to any issues particular to the Department of Defense. Order, ECF No. 23. On July 10, Defendants submitted a Supplemental Brief, notifying the Court of certain factual developments since the July 7 hearing. First, Defendants represented that the Commission “no longer intends to use the DOD SAFE system to receive information from the states.” Third Decl. of Kris W. Kobach, ECF No. 24-1 (“Third Kobach Decl.”), ¶ 1. Instead, Defendants stated that the Director of White House Information Technology was working to “repurpos[e] an existing system that regularly accepts personally identifiable information through a secure, encrypted computer application,” and that this new system was expected to be “fully functional by 6:00pm EDT [on July 10, 2017].” *Id.* Second, Defendants provided the Court with a follow-up communication sent to the states, directing election officials to “hold on submitting any data” until this Court resolved Plaintiff’s motion for injunctive relief. *Id.*, Ex. A. In light of these developments, Plaintiff moved to further amend the complaint pursuant to Federal Rule of Civil Procedure 15(a)(2), to name as additional defendants the Director of White House Information Technology, the Executive Committee for Presidential Information Technology, and the United States Digital Service, which the Court granted. Pl.’s Mot. to Am. Compl., ECF No. 30; Order, ECF No. 31.

Given the “substantial changes in factual circumstances” since this action was filed, the Court directed Plaintiff to file an amended motion for injunctive relief. Order, ECF No. 31. Plaintiff filed the amended motion on July 13, seeking to enjoin Defendants from “collecting voter roll data from states and state election officials” and to require

Defendants to “disgorge any voter roll data already collected or hereafter received.” Proposed Order, ECF No. 35-6, at 1–2. Defendants’ response supplied additional information about how the voter roll data would be collected and stored by the “repurposed” White House computer system. *See* Decl. of Charles Christopher Herndon, ECF No. 38-1 (“Herndon Decl.”), ¶¶ 3–6. According to Defendants, the new system requires state officials to request an access link, which then allows them to upload data to a “server within the domain electionintergrity.whitehouse.gov.” *Id.* ¶ 4. Once the files have been uploaded, “[a]uthorized members of the Commission will be given access” with “dedicated laptops” to access the data through a secure White House network. *Id.* ¶ 4–5. Defendants represent that this process will only require the assistance of “a limited number of technical staff from the White House Office of Administration” *Id.* ¶ 6. Finally, Defendants represented that the voter roll data uploaded to the SAFE system by the state of Arkansas—the only voter roll information known to the Court that has been transferred in response to the Commission’s request—“ha[d] been deleted without ever having been accessed by the Commission.” *Id.* ¶ 7.

II. LEGAL STANDARD

Preliminary injunctive relief, whether in the form of temporary restraining order or a preliminary injunction, is “an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief.” *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011) (quoting *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008)); *see also Mazurek v. Armstrong*, 520 U.S. 968, 972 (1997) (“[A] preliminary injunction is an extraordinary and drastic remedy, one that should not be granted unless the movant, by a clear showing, carries the burden of persuasion.” (emphasis in original;

quotation marks omitted)). A plaintiff seeking preliminary injunctive relief “must establish [1] that he is likely to succeed on the merits, [2] that he is likely to suffer irreparable harm in the absence of preliminary relief, [3] that the balance of equities tips in his favor, and [4] that an injunction is in the public interest.” *Aamer v. Obama*, 742 F.3d 1023, 1038 (D.C. Cir. 2014) (quoting *Sherley*, 644 F.3d at 392 (quoting *Winter*, 555 U.S. at 20) (alteration in original; quotation marks omitted)). When seeking such relief, “the movant has the burden to show that all four factors, taken together, weigh in favor of the injunction.” *Abdullah v. Obama*, 753 F.3d 193, 197 (D.C. Cir. 2014) (quoting *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1292 (D.C. Cir. 2009)). “The four factors have typically been evaluated on a ‘sliding scale.’” *Davis*, 571 F.3d at 1291 (citation omitted). Under this sliding-scale framework, “[i]f the movant makes an unusually strong showing on one of the factors, then it does not necessarily have to make as strong a showing on another factor.” *Id.* at 1291–92.³

III. DISCUSSION

A. Article III Standing

As a threshold matter, the Court must determine whether Plaintiff has standing to

³ The Court notes that it is not clear whether this circuit’s sliding-scale approach to assessing the four preliminary injunction factors survives the Supreme Court’s decision in *Winter*. See *Save Jobs USA v. U.S. Dep’t of Homeland Sec.*, 105 F. Supp. 3d 108, 112 (D.D.C. 2015). Several judges on the United States Court of Appeals for the District of Columbia Circuit (“D.C. Circuit”) have “read *Winter* at least to suggest if not to hold ‘that a likelihood of success is an independent, free-standing requirement for a preliminary injunction.’” *Sherley*, 644 F.3d at 393 (quoting *Davis*, 571 F.3d at 1296 (concurring opinion)). However, the D.C. Circuit has yet to hold definitively that *Winter* has displaced the sliding-scale analysis. See *id.*; see also *Save Jobs USA*, 105 F. Supp. 3d at 112. In any event, this Court need not resolve the viability of the sliding-scale approach today, as it finds that Plaintiff has failed to show a likelihood of success on the merits and irreparable harm, and that the other preliminary injunction factors are in equipoise.

bring this lawsuit. Standing is an element of this Court’s subject-matter jurisdiction under Article III of the Constitution, and requires, in essence, that a plaintiff have “a personal stake in the outcome of the controversy” *Warth v. Seldin*, 422 U.S. 490, 498 (1975). Consequently, a plaintiff cannot be a mere bystander or interested third-party, or a self-appointed representative of the public interest; he or she must show that defendant’s conduct has affected them in a “personal and individual way.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992). The familiar requirements of Article III standing are:

(1) that the plaintiff have suffered an “injury in fact”—an invasion of a judicially cognizable interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) that there be a causal connection between the injury and the conduct complained of—the injury must be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court; and (3) that it be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Bennett v. Spear, 520 U.S. 154, 167 (1997) (citing *Lujan*, 504 U.S. at 560–61). The parties have briefed three theories of standing. Two are based on Plaintiff’s own interests—for injuries to its informational interests and programmatic public interest activities—while the third is based on the interests of Plaintiff’s advisory board members. This latter theory fails, but the first two succeed, for the reasons detailed below.

1. Associational Standing

An organization may sue to vindicate the interests of its members. To establish this type of “associational” standing, Plaintiff must show that “(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization’s purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit.” *Ass’n of Flight Attendants-CWA, AFL-CIO v. U.S. Dep’t of Transp.*, 564 F.3d 462, 464 (D.C. Cir. 2009) (internal

quotation marks omitted). Needless to say, Plaintiff must also show that it has “members” whose interests it is seeking to represent. To the extent Plaintiff does not have a formal membership, it may nonetheless assert organizational standing if “the organization is the functional equivalent of a traditional membership organization.” *Fund Democracy, LLC v. S.E.C.*, 278 F.3d 21, 25 (D.C. Cir. 2002). For an organization to meet the test of functional equivalency, “(1) it must serve a specialized segment of the community; (2) it must represent individuals that have all the ‘indicia of membership’ including (i) electing the entity’s leadership, (ii) serving in the entity, and (iii) financing the entity’s activities; and (3) its fortunes must be tied closely to those of its constituency.” *Washington Legal Found. v. Leavitt*, 477 F. Supp. 2d 202, 208 (D.D.C. 2007) (citing *Fund Democracy*, 278 F.3d at 25).

Plaintiff has submitted the declarations of nine advisory board members from six jurisdictions representing that the disclosure of their personal information—including “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”—will cause them immediate and irreparable harm. ECF No. 35-3, Exs. 7–15. The parties disagree on whether these advisory board members meet the test of functional equivalency. For one, Plaintiff’s own website concedes that the organization “ha[s] no clients, no customers, and no shareholders” *See* About EPIC, <http://epic.org/epic/about.html> (last accessed July 20, 2017). Contrary to this assertion, however, Plaintiff has proffered testimony to the effect that advisory board members exert substantial influence over the affairs of the organization, including by influencing the matters in which the organization participates, and that advisory board members are

expected to contribute to the organization, either financially or by offering their time and expertise. Hr’g Tr. 16:1–18:19; *see also* Decl. of Marc Rotenberg, ECF No. 35-5, Ex. 38, ¶¶ 8–12. In the Court’s view, however, the present record evidence is insufficient for Plaintiff to satisfy its burden with respect to associational standing. There is no evidence that members are *required* to finance the activities of the organization; that they have any role in electing the leadership of the organization; or that their fortunes, as opposed to their policy viewpoints, are “closely tied” to the organization. *See id.*; About EPIC, <http://epic.org/epic/about.html> (last accessed July 20, 2017) (“EPIC *works closely with a distinguished advisory board, with expertise in law, technology and public policy. . . . EPIC is a 501(c)(3) nonprofit. We have no clients, no customers, and no shareholders. We need your support.*” (emphasis added)); *see also Elec. Privacy Info. Ctr. v. U.S. Dep’t of Educ.*, 48 F. Supp. 3d 1, 22 (D.D.C. 2014) (“defendant raises serious questions about whether EPIC is an association made up of members that may avail itself of the associational standing doctrine”).

Furthermore, even if the Court were to find that Plaintiff is functionally equivalent to a membership organization, the individual advisory board members who submitted declarations do not have standing to sue in their own capacities. First, these individuals are registered voters in states that have declined to comply with the Commission’s request for voter roll information, and accordingly, they are not under imminent threat of either the statutory or Constitutional harms alleged by Plaintiff. *See Am. Opp’n Mem.*, at 13. Second, apart from the alleged violations of the advisory board members’ Constitutional privacy rights—the existence of which the Court assumes for purposes of its standing analysis, *see Parker v. D.C.*, 478 F.3d 370, 378 (D.C. Cir. 2007), *aff’d sub nom. D.C. v. Heller*, 554 U.S.

570 (2008)—Plaintiff has failed to proffer a theory of individual harm that is “actual or imminent, [and not merely] conjectural or hypothetical . . . [.]” *Bennett*, 520 U.S. at 167. Plaintiff contends that the disclosure of sensitive voter roll information would cause immeasurable harm that would be “impossible to contain . . . after the fact.” Pl.’s Am. Mem., at 13. The organization also alleges that the information may be susceptible to appropriation for unspecified “deviant purposes.” *Id.* (internal citations omitted). However, Defendants have represented that they are only collecting voter information that is already publicly available under the laws of the states where the information resides; that they have only requested this information and have not demanded it; and Defendants have clarified that such information, to the extent it is made public, will be de-identified. *See supra* at [•]. All of these representations were made to the Court in sworn declarations, and needless to say, the Court expects that Defendants shall strictly abide by them.

Under these factual circumstances, however, the only practical harm that Plaintiff’s advisory board members would suffer, assuming their respective states decide to comply with the Commission’s request in the future, is that their already publicly available information would be rendered more easily accessible by virtue of its consolidation on the computer systems that would ultimately receive this information on behalf of the Commission. It may be true, as Plaintiff contends, that there are restrictions on how “publicly available” voter information can be obtained in the ordinary course, such as application and notification procedures. Hr’g Tr. 8:2–21. But even granting the assumption that the Commission has or will receive information in a manner that bypasses these safeguards, the only way that such information would be rendered more accessible for nefarious purposes is if the Court further assumes that either the Commission systems are

more susceptible to compromise than those of the states, or that the de-identification process eventually used by Defendants will not sufficiently anonymize the information when it is publicized. Given the paucity of the record before the Court, this sequence of events is simply too attenuated to confer standing. At most, Plaintiff has shown that its members will suffer an increased *risk* of harm if their already publicly available information is collected by the Commission. But under the binding precedent of the Supreme Court, an increased risk of harm is insufficient to confer standing; rather, the harm must be “certainly impending.” *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1143 (2013). Indeed, on this basis, two district courts in this circuit have concluded that even the disclosure of *confidential, identifiable* information is insufficient to confer standing until that information is or is about to be used by a third-party to the detriment of the individual whose information is disclosed. *See In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014); *Welborn v. IRS*, 218 F. Supp. 3d 64, 77 (D.D.C. 2016). In sum, the mere increased risk of disclosure stemming from the collection and eventual, anonymized disclosure of already publicly available voter roll information is insufficient to confer standing upon Plaintiff’s advisory board members. Consequently, for all of the foregoing reasons, Plaintiff has failed to show that it has associational standing to bring this lawsuit.⁴

⁴ This obviates the need to engage in a merits analysis of Plaintiff’s alleged Constitutional privacy right claims, which are based on the individual claims of its advisory board members. *See generally* Pl.’s Am. Mem., at 30. Nonetheless, even if the Court were to reach this issue, it would find that Plaintiff is unlikely to succeed on these claims because the D.C. Circuit has expressed “grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information.” *Am. Fed’n of Gov’t Emps., AFL-CIO v. Dep’t of Hous. & Urban Dev.*, 118 F.3d 786, 791 (D.C. Cir. 1997).

2. Informational Standing

In order to establish informational standing, Plaintiff must show that “(1) it has been deprived of information that, on its interpretation, a statute requires the government or a third party to disclose to it, and (2) it suffers, by being denied access to that information, the type of harm Congress sought to prevent by requiring disclosure.” *Friends of Animals v. Jewell*, 828 F.3d 989, 992 (D.C. Cir. 2016). “[A] plaintiff seeking to demonstrate that it has informational standing generally ‘need not allege any additional harm beyond the one Congress has identified.’” *Id.* (citing *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1544 (2016)). Plaintiff has brought suit under the APA, for the failure of one or more federal agencies to comply with Section 208 of the E-Government Act. That provision mandates that before “initiating a new collection of information,” an agency must “conduct a privacy impact assessment,” “ensure the review of the privacy impact assessment by the Chief Information Officer,” and “if practicable, after completion of the review . . . , make 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). An enumerated purpose of the E-Government Act is “[t]o make the Federal Government more transparent and accountable.” *Id.* § 2(b)(9).

Plaintiff satisfies both prongs of the test for informational standing. First, it has espoused a view of the law that entitles it to information. Namely, Plaintiff contends that Defendants are engaged in a new collection of information, and that a cause of action is available under the APA to force their compliance with the E-Government Act and to require the disclosure of a Privacy Impact Assessment. Second, Plaintiff contends that it has suffered the very injuries meant to be prevented by the disclosure of information

pursuant to the E-Government Act—lack of transparency and the resulting lack of opportunity to hold the federal government to account. This injury is particular to Plaintiff, given that it is an organization that was “established . . . to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.” About EPIC, <https://www.epic.org/epic/about.html> (last accessed July 20, 2017). Plaintiff, moreover, engages in government outreach by “speaking before Congress and judicial organizations about emerging privacy and civil liberties issues[,]” *id.*, and uses information it obtains from the government to carry out its mission to educate the public regarding privacy issues, Hr’g Tr. 20:12–23.

Defendants have contested Plaintiff’s informational standing, citing principally to the D.C. Circuit’s analysis in *Friends of Animals*. See Am. Opp’n Mem., at 14–20. There, the court held that plaintiff, an environmental organization, did not have informational standing under a statute that required the Department of the Interior (“DOI”), *first*, to make certain findings regarding whether the listing of a species as endangered is warranted within 12 months of determining that a petition seeking that relief “presents substantial scientific or commercial information,” and *second*, after making that finding, to publish certain information in the Federal Register, including under some circumstances, a proposed regulation, or an “evaluation of the reasons and data on which the finding is based.” *Friends of Animals*, 828 F.3d at 990–91 (internal quotation marks omitted) (citing 16 U.S.C. § 1533(b)(3)(B)). For example, part of the statute in *Friends of Animals* required that:

(B) Within 12 months after receiving a petition that is found under subparagraph (A) to present substantial information indicating that the petitioned action may be warranted, the Secretary shall make one of the following findings: . . .

(ii) The petitioned action is warranted, in which case the Secretary shall promptly publish in the Federal Register a general notice and the complete text of a proposed regulation to implement such action in accordance with paragraph (5).

16 U.S.C. § 1533(b)(3)(B)(ii). At the time plaintiff brought suit, the 12-month period had elapsed, but the DOI had yet to make the necessary findings, and consequently had not published any information in the Federal Register. In assessing plaintiff's informational standing, the D.C. Circuit focused principally on the structure of the statute that allegedly conferred on plaintiff a right to information from the federal government. *Friends of Animals*, 828 F.3d at 993. Solely on that basis, the court determined that plaintiff was not entitled to information because a right to information (e.g., a proposed regulation under subsection (B)(ii) or an evaluation under subsection (B)(iii)) arose only *after* the DOI had made one of the three findings envisioned by the statute. True, the DOI had failed to make the requisite finding within 12 months. But given the statutorily prescribed sequence of events, plaintiff's challenge was in effect to the DOI's failure to make such a finding, rather than to its failure to disclose information, given that the obligation to disclose information only arose after a finding had been made. As such, the D.C. Circuit concluded that plaintiff lacked informational standing.

The statutory structure here, however, is quite different. The relevant portion of Section 208 provides the following:

(b) PRIVACY IMPACT ASSESSMENTS.—

(1) RESPONSIBILITIES OF AGENCIES.

(A) IN GENERAL.—An agency shall take actions described under subparagraph (B) before

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) 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.

(B) AGENCY ACTIVITIES.—To the extent required under subparagraph (A), each agency shall—

(i) conduct 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.

E-Government Act, § 208(b). As this text makes clear, the statutorily prescribed sequence of events here is reversed from the sequence at issue in *Friends of Animals*. There, the DOI was required to disclose information only *after* it had made one of three “warranted” findings; it had not made any finding, and accordingly, was not obligated to disclose any information. Here, the statute mandates that an “agency *shall* take actions described under subparagraph (B) *before* . . . initiating a new collection of information . . .” *Id.* (emphasis added). Subparagraph (B) in turn requires the agency to conduct a Privacy Impact Assessment, to have it reviewed by the Chief Information Officer or his equivalent, and to publish the assessment, if practicable. The statute, given its construction, requires all three of these events, including the public disclosure of the assessment, to occur *before* the

agency initiates a new collection of information. Assuming that the other facets of Plaintiff's interpretation of the law are correct—namely, that Defendants are engaged in a new collection of information subject to the E-Government Act, that judicial review is available under the APA, and that disclosure of a privacy assessment is “practicable”—then Plaintiff is presently entitled to information pursuant to the E-Government Act, because the disclosure of information was already supposed to have occurred; that is, a Privacy Impact Assessment should have been made publicly available before Defendants systematically began collecting voter roll information. Accordingly, unlike in *Friends of Animals*, a review of the statutory text at issue in this litigation indicates that, under Plaintiff's interpretation of the law, Defendants have already incurred an obligation to disclose information.

Defendants make three further challenges to Plaintiff's informational standing, none of which are meritorious. First, Defendants contend that Plaintiff lacks standing because its informational injury is merely a “generalized grievance,” and therefore insufficient to confer standing. Am. Opp'n Mem., at 15 (citing *Judicial Watch, Inc. v. FEC*, 180 F.3d 277, 278 (D.C. Cir. 1999)). Plainly, the E-Government Act entitles the public generally to the disclosure of Privacy Impact Assessments, but that does not mean that the informational injury in this case is not particular to Plaintiff. As already noted, Plaintiff is a public-interest organization that focuses on privacy issues, and uses information gleaned from the government to educate the public regarding privacy, and to petition the government regarding privacy law. *See supra* at [•]. Accordingly, the informational harm in this case, as it relates to Plaintiff, is “concrete and particularized.” Moreover, the reality of statutes that confer informational standing is that they are often not targeted at a

particular class of individuals, but rather provide for disclosure to the public writ large. *See, e.g., Friends of Animals*, 824 F.3d at 1041 (finding that public interest environmental organization had standing under statutory provision that required the Department of the Interior to publish certain information in the Federal Register). Even putting aside the particularized nature of the informational harm alleged in this action, however, the fact that a substantial percentage of the public is subject to the same harm does not automatically render that harm inactionable. As the Supreme Court observed in *Akins*: “Often the fact that an interest is abstract and the fact that it is widely shared go hand in hand. But their association is not invariable, and where a harm is concrete, though widely shared, the Court has found ‘injury in fact.’” *FEC v. Akins*, 524 U.S. 11, 24 (1998). The Court went on to hold, in language that is particularly apt under the circumstances, that “the informational injury at issue . . . , directly related to voting, the most basic of political rights, is sufficiently concrete and specific” *Id.* at 24–25.

Defendants next focus on the fact that the information sought does not yet exist in the format in which it needs to be disclosed (i.e., as a Privacy Impact Assessment). Am. Opp’n Mem., at 17. In this vein, they claim that *Friends of Animals* stands for the proposition that the government cannot be required to create information. The Court disagrees with this interpretation of *Friends of Animals*, and moreover, Defendants’ view of the law is not evident in the controlling Supreme Court and D.C. Circuit precedents. As already detailed, the court in *Friends of Animals* looked solely to the statutory text to determine whether an obligation to disclose had been incurred. No significance was placed by the D.C. Circuit on the fact that, if there were such an obligation, the federal government would potentially be required to “create” the material to be disclosed (in that case, either a

proposed regulation, or an evaluative report). Furthermore, *Friends of Animals* cited two cases, one by the D.C. Circuit and the other by the Supreme Court, as standing for the proposition that plaintiffs have informational standing to sue under “statutory provisions that guarantee[] a right to receive information *in a particular form.*” *Friends of Animals*, 828 F.3d at 994 (emphasis added; citing *Zivotofsky ex rel. Ari Z. v. Sec’y of State*, 444 F.3d 614, 615–19 (D.C. Cir. 2006), and *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373–75 (1982)). Furthermore, in *Public Citizen*, the Supreme Court found that plaintiff had informational standing to sue under FACA, and thereby seek the disclosure of an advisory committee charter and other materials which FACA requires advisory committees to create and make public. Presumably those materials did not exist, given defendants’ position that the committee was not subject to FACA, and in any event, the Court made no distinction on this basis. *Pub. Citizen v. U.S. Dep’t of Justice*, 491 U.S. 440, 447 (1989). And in *Akins*, the information sought was not in defendants’ possession, as the entire lawsuit was premised on requiring defendant to take enforcement action to obtain that information. 524 U.S. at 26. Ultimately, the distinction between information that already exists, and information that needs to be “created,” if not specious, strikes the Court as an unworkable legal standard. Information does not exist in some ideal form. When the government discloses information, it must always first be culled, organized, redacted, reviewed, and produced. Sometimes the product of that process, as under the Freedom of Information Act, is a production of documents, perhaps with an attendant privilege log. *See, e.g., Judicial Watch, Inc. v. Food & Drug Admin.*, 449 F.3d 141, 146 (D.C. Cir. 2006) (explaining the purpose of a *Vaughn* index). Here, Congress has mandated that disclosure take the form of a Privacy Impact Assessment, and that is what Plaintiff has standing to

seek, regardless of whether an agency is ultimately required to create the report.

Lastly, Defendants contend that Plaintiff lacks informational standing because Section 208 only requires the publication of a Privacy Impact Statement if doing so is “practicable.” Am. Opp’n Mem., at 17 n.2. As an initial matter, Defendants have at no point asserted that it would be impracticable to create and publish a Privacy Impact Assessment; rather, they have rested principally on their contention that they are not required to create or disclose one because Plaintiff either lacks standing, or because the E-Government Act and APA only apply to federal agencies, which are not implicated by the collection of voter roll information. Accordingly, whatever limits the word “practicable” imposes on the disclosure obligations of Section 208, they are not applicable in this case, and therefore do not affect Plaintiff’s standing to bring this lawsuit. As a more general matter, however, the Court disagrees with Defendants’ view that merely because a right to information is in some way qualified, a plaintiff lacks informational standing to seek vindication of that right. For this proposition, Defendants again cite *Friends of Animals*, contending that the D.C. Circuit held that “informational standing only exists if [the] statute ‘guaranteed a right to receive information in a particular form’” *Id.* (citing *Friends of Animals*, 828 F.3d at 994). That is not what the D.C. Circuit held; rather that language was merely used to describe two other cases, *Haven* and *Zivotofsky*, in which the Supreme Court and D.C. Circuit determined that plaintiffs had informational standing. *See supra* at [•]. One only need to look toward the Freedom of Information Act, under which litigants undoubtedly have informational standing despite the fact that the Act in no way provides an unqualified right to information, given its numerous statutory exemptions. *See Zivotofsky*, 444 F.3d at 618. Moreover, the available guidance indicates that the qualifier “practicable” was meant

to function similarly to the exemptions under the Freedom of Information Act, and is therefore not purely discretionary. *See* M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003) (“Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment. *Such information shall be protected and handled consistent with the Freedom of Information Act . . .*” (footnote omitted; emphasis added)). Accordingly, for all of the foregoing reasons, the Court concludes that Plaintiff has satisfied its burden at this stage regarding its informational standing to seek the disclosure of a Privacy Impact Assessment pursuant to Section 208 of the E-Government Act.

Moreover, because the Court assumes the merits of Plaintiff’s claims for standing purposes, the Court also finds that Plaintiff has informational standing with respect to its FACA claim, which likewise seeks the disclosure of a Privacy Impact Assessment. *Judicial Watch, Inc. v. U.S. Dep’t of Commerce*, 583 F.3d 871, 873 (D.C. Cir. 2009) (“Here the injury requirement is obviously met. In the context of a FACA claim, an agency’s refusal to disclose information that the act requires be revealed constitutes a sufficient injury.”)

3. *Organizational Standing Under PETA*

For similar reasons to those enumerated above with respect to informational standing, the Court also finds that Plaintiff has organizational standing under *PETA v. USDA*, 797 F.3d 1087 (D.C. Cir. 2015). In this circuit, an organization may establish standing if it has “suffered a concrete and demonstrable injury to its activities, mindful that,

under our precedent, a mere setback to . . . abstract social interests is not sufficient.” *Id.* at 1093 (internal quotation marks and alterations omitted) (citing *Am. Legal Found. v. FCC*, 808 F.2d 84, 92 (D.C. Cir. 1987) (“The organization must allege that discrete programmatic concerns are being directly and adversely affected by the defendant’s actions.”)). “Making this determination is a two-part inquiry—we ask, first, whether the agency’s action or omission to act injured the organization’s interest and, second, whether the organization used its resources to counteract that harm.” *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 919 (D.C. Cir. 2015) (internal quotation marks and alterations omitted). In *PETA*, the D.C. Circuit found that an animal rights organization had suffered a “denial of access to bird-related . . . information including, in particular, investigatory information, and a means by which to seek redress for bird abuse” *PETA*, 797 F.3d at 1095. This constituted a “cognizable injury sufficient to support standing” because the agency’s failure to comply with applicable regulations had impaired PETA’s ability to bring “violations to the attention of the agency charged with preventing avian cruelty and [to] continue to educate the public.” *Id.*

Under the circumstances of this case, Plaintiff satisfies the requirements for organizational standing under *PETA*. Plaintiff has a long-standing mission to educate the public regarding privacy rights, and engages in this process by obtaining information from the government. Pl.’s Reply Mem. at 17 (“EPIC’s mission includes, in particular, educating the public about the government’s record on voter privacy and promoting safeguards for personal voter data.”). Indeed, Plaintiff has filed Freedom of Information Act requests in this jurisdiction seeking the disclosure of the same type of information, Privacy Impact Assessments, that it claims has been denied in this case. *See, e.g., Elec. Privacy Info. Ctr.*

v. DEA, 208 F. Supp. 3d 108, 110 (D.D.C. 2016). Furthermore, Plaintiff’s programmatic activities—educating the public regarding privacy matters—have been impaired by Defendants’ alleged failure to comply with Section 208 of the E-Government Act, since those activities routinely rely upon access to information from the federal government. *See* Hr’g Tr. at 20:8–16. This injury has required Plaintiff to expend resources by, at minimum, seeking records from the Commission and other federal entities concerning the collection of voter data. *See* Decl. of Eleni Kyriakides, ECF No. 39-1, ¶ 6. Accordingly, Plaintiff has organizational standing under the two-part test sanctioned by the D.C. Circuit in *PETA*.

B. Likelihood of Success on the Merits

Having assured itself of Plaintiff’s standing to bring this lawsuit, the Court turns to assess the familiar factors for determining whether a litigant is entitled to preliminary injunctive relief; in this case, a temporary restraining order and preliminary injunction. The first, and perhaps most important factor, is Plaintiff’s likelihood of success on the merits.

The E-Government Act does not provide for a private cause of action, and accordingly, Plaintiff has sought judicial review pursuant to Section 702 of the APA. *See Greenspan v. Admin. Office of the United States Courts*, No. 14CV2396 JTM, 2014 WL 6847460, at *8 (N.D. Cal. Dec. 4, 2014). Section 704 of the APA, in turn, limits judicial review to “final agency action for which there is no other adequate remedy” As relevant here, the reviewing court may “compel agency action unlawfully withheld or unreasonably delayed.” 5 U.S.C. § 706(1). The parties principally disagree over whether any “agency” is implicated in this case such that there could be an “agency action” subject to this Court’s review. *See* Pl.’s Am. Mem., at 19–30; Am. Opp’n Mem., at 20–33.

“Agency” is broadly defined by the APA to include “each authority of the

Government of the United States, whether or not it is within or subject to review by another agency” 5 U.S.C. § 551(1). The statute goes on to exclude certain components of the federal government, including Congress and the federal courts, but does not by its express terms exclude the President, or the Executive Office of the President (“EOP”). *Id.* Nonetheless, the Supreme Court has concluded that the President is exempted from the reach of the APA, *Franklin v. Massachusetts*, 505 U.S. 788, 800–01 (1992), and the D.C. Circuit has established a test for determining whether certain bodies within the Executive Office of the President are sufficiently close to the President as to also be excluded from APA review, *see Armstrong v. Exec. Office of the President*, 90 F.3d 553, 558 (D.C. Cir. 1996) (citing *Meyer v. Bush*, 981 F.2d 1288 (D.C. Cir. 1993)). In determining whether the Commission is an “agency,” or merely an advisory body to the President that is exempted from APA review, relevant considerations include “whether the entity exercises substantial independent authority,” “whether the entity’s sole function is to advise and assist the President,” “how close operationally the group is to the President,” “whether it has a self-contained structure,” and “the nature of its delegated authority.” *Citizens for Responsibility & Ethics in Washington v. Office of Admin.*, 566 F.3d 219, 222 (D.C. Cir. 2009) (“CREW”) (internal quotation marks omitted). The most important consideration appears to be whether the “entity in question wielded substantial authority independently of the President.” *Id.*

The record presently before the Court is insufficient to demonstrate that the Commission is an “agency” for purposes of the APA. First, the Executive Order indicates that the Commission is purely advisory in nature, and that it shall disband shortly after it delivers a report to the President. No independent authority is imbued upon the

Commission by the Executive Order, and there is no evidence that it has exercised any independent authority that is unrelated to its advisory mission. Defendants' request for information is just that—a request—and there is no evidence that they have sought to turn the request into a demand, or to enforce the request by any means. Furthermore, the request for voter roll information, according to Defendants, is ancillary to the Commission's stated purpose of producing an advisory report for the President regarding voting processes in federal elections. The Executive Order does provide that other federal agencies "shall endeavor to cooperate with the Commission," and 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." Exec. Order § 7(a). Nonetheless, Defendants have represented that the GSA's role is currently expected to be limited to specific "administrative support like arranging travel for the members" of the Commission, and that no other federal agencies are "cooperating" with the Commission. Hr'g Tr. at 27:25–28:6; 30:10–13. Finally, although Commissioner Christy McCormick of the Election Assistance Commission is a member of the Commission, there is currently no record evidence that she was substantially involved in the decision to collect voter information, or that her involvement in some fashion implicated the Election Assistance Commission, which is a federal agency. Hr'g Tr. 28:24–30:4; *cf. Judicial Watch, Inc. v. Nat'l Energy Policy Dev. Grp.*, 219 F. Supp. 2d 20, 39–40 (D.D.C. 2002) (citing *Ryan v. Dep't of Justice*, 617 F.2d 781 (D.C. Cir. 1980)).

This would have ended the inquiry, but for the revelation during the course of these proceedings that the SAFE system, which the Commission had intended for states to use to transmit voter roll information, is operated by a component of the Department of

Defense. Moreover, the only voter roll information transferred to date resided on the SAFE system, and consequently was stored on a computer system operated by the Department of Defense. Given these factual developments, the Department of Defense—a federal agency—was added as a defendant to this lawsuit. *See* Am. Compl., ECF No. 21, ¶¶ 37–42. Shortly after that occurred, however, Defendants changed gears, and represented that “[i]n order not to impact the ability of other customers to use the [SAFE] site, the Commission has decided to use alternative means for transmitting the requested data.” ECF No. 24, at 1. In lieu of the SAFE system, Defendants had the Director of White House Information Technology (“DWHIT”) repurpose “an existing system that regularly accepts personally identifiable information through a secure, encrypted computer application within the White House Information Technology enterprise.” *Id.* Furthermore, Defendants have represented that the data received from the State of Arkansas via the SAFE system has been deleted, “without ever having been accessed by the Commission.” Herndon Decl. ¶ 7. Accordingly, while the legal dispute with respect to the use of the SAFE system by Defendants to collect at least some voter roll information may not be moot—data was in fact collected before a Privacy Impact Assessment was conducted pursuant to the E-Government Act—that potential legal violation does not appear to be a basis for the prospective injunctive relief sought by Plaintiff’s amended motion for injunctive relief; namely, the prevention of the further collection of voter roll information by the Commission. In any event, Plaintiff has not pursued the conduct of the Department of Defense as a basis for injunctive relief.

Given the change of factual circumstances, the question now becomes whether any of the entities that will be involved in administering the “repurposed” White House system

are “agencies” for purposes of APA review. One candidate is the DWHIT. According to the Presidential Memorandum establishing this position, the “Director of White House Information Technology, on behalf of the President, shall have the 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 the EOP.” Mem. on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology (“DWHIT Mem.”), § 1, *available at* <https://www.gpo.gov/fdsys/pkg/DCPD-201500185/pdf/DCPD-201500185.pdf> (last accessed July 16, 2017). The DWHIT is part of the White House Office, *id.* § 2(a)(ii), a component of the EOP “whose members assist the President with those tasks incidental to the office.” *Alexander v. F.B.I.*, 691 F. Supp. 2d 182, 186 (D.D.C. 2010), *aff’d*, 456 F. App’x 1 (D.C. Cir. 2011); *see also* Herndon Decl. ¶ 1. According to the Memorandum, the DWHIT “shall ensure the effective use of information resources and information systems provided to the President, Vice President, and EOP in order to improve mission performance, and shall have the appropriate authority to promulgate all necessary procedures and rules governing these resources and systems.” DWHIT Mem., § 2(c). The DWHIT is also responsible for providing “policy coordination and guidance” for a group of other entities that provide information technology services to the President, Vice President, and the EOP, known as the “Presidential Information Technology Community.” *Id.* § 2(a), (c). Furthermore, the DWHIT may “advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director’s duties under this memorandum.” *Id.* § 2(d).

Taken as a whole, the responsibilities of the DWHIT based on the present record

amount to providing operational and administrative support services for information technology used by the President, Vice President, and close staff. Furthermore, to the extent there is coordination with other federal agencies, the purpose of that coordination is likewise to ensure the sufficiency and quality of information services provided to the President, Vice President, and their close staff. Given the nature of the DWHIT's responsibilities and its proximity to the President and Vice President, it is not an agency for the reasons specified by the D.C. Circuit in *CREW* with respect to the Office of Administration ("OA"). In that case, the D.C. Circuit held that the OA was not an "agency" under FOIA⁵ because "nothing in the record indicate[d] that OA performs or is authorized to perform tasks other than operational and administrative support for the President and his staff" *CREW*, 566 F.3d at 224. Relying on its prior holding in *Sweetland*, the court held that where an entity within the EOP, like the DWHIT, provides to the President and his staff "only operational and administrative support . . . it lacks the substantial

⁵ Plaintiff argues that *CREW* and similar cases by the D.C. Circuit interpreting whether an entity is an agency for purposes of FOIA are not applicable to determining whether an entity is an agency for purposes of the APA. See Pl.'s Reply Mem. at 2. The Court disagrees. The D.C. Circuit established the "substantial independent authority" test in *Soucie*, a case that was brought under FOIA, but at a time when the definition of "agency" for FOIA purposes mirrored the APA definition. In that case, the D.C. Circuit held that "the APA apparently confers agency status on any administrative unit with *substantial independent authority* in the exercise of specific functions." *Soucie v. David*, 448 F.2d 1067, 1073 (D.C. Cir. 1971) (emphasis added); *Meyer*, 981 F.2d at 1292 n.1 ("[b]efore the 1974 Amendments, FOIA simply had adopted the APA's definition of agency"); see also *Dong v. Smithsonian Inst.*, 125 F.3d 877, 881 (D.C. Cir. 1997) ("[o]ur cases have followed the same approach, requiring that an entity exercise substantial independent authority before it can be considered an agency for § 551(1) purposes"—that is, the section that defines the term "agency" for purposes of the APA). The *CREW* court applied the "substantial independent authority" test, and the Court sees no basis to hold that the reasoning of *CREW* is not dispositive of DWHIT's agency status in this matter.

independent authority we have required to find an agency covered by FOIA” *Id.* at 223 (citing *Sweetland v. Walters*, 60 F.3d 852, 854 (D.C. Cir. 1995)). This conclusion was unchanged by the fact that the OA, like the DWHIT here, provides support for other federal agencies to the extent they “work at the White House complex in support of the President and his staff.” *Id.* at 224. Put differently, the fact that the DWHIT coordinates the information technology support provided by other agencies for the President, Vice President, and their close staff, does not change the ultimate conclusion that the DWHIT is not “authorized to perform tasks other than operational and administrative support for the President and his staff,” which means that the DWHIT “lacks substantial independent authority and is therefore not an agency” *Id.* However, to the extent that DWHIT’s responsibilities expand either formally or organically, as a result of its newfound responsibilities in assisting the Commission, this determination may need to be revisited in the factual context of this case.

The other candidates for “agency action” proposed by Plaintiff fare no better. The Executive Committee for Presidential Information Technology and the U.S. Digital Service, even if they were agencies, “will have no role in th[e] data collection process.” Herndon Decl. ¶ 6. According to Defendants, apart from the DWHIT, the only individuals who will be involved in the collection of voter roll information are “a limited number of . . . technical staff from the White House Office of Administration.” *Id.* Finally, Plaintiff contends that the entire EOP is a “parent agency,” and that as a result, the activities of its components, including those of the DWHIT and the Commission, are subject to APA review. However, this view of the EOP has been expressly rejected by the D.C. Circuit and is at odds with the practical reality that the D.C. Circuit has consistently analyzed the

agency status of EOP components on a component-by-component basis. *United States v. Espy*, 145 F.3d 1369, 1373 (D.C. Cir. 1998) (“it has never been thought that the whole Executive Office of the President could be considered a discrete agency under FOIA”). Accordingly, at the present time and based on the record before the Court, it appears that there is no “agency,” as that term is understood for purposes of the APA, that is involved in the collection of voter roll information on behalf of the Commission. Because there is no apparent agency involvement at this time, the Court concludes that APA review is presently unavailable in connection with the collection of voter roll information by the Commission.

The last remaining avenue of potential legal redress is pursuant to FACA. Plaintiff relies on Section 10(b) of FACA as a means to seek the disclosure of a Privacy Impact Assessment, as required under certain circumstances by the E-Government Act. *See* Am. Compl, ECF No. 33, ¶¶ 73–74. That section provides that an advisory committee subject to FACA must make publicly available, unless an exception applies under FOIA, “the records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [the] advisory committee” 5 U.S.C. app. 2 § 10(b). The flaw with this final approach, however, is that FACA itself does not require Defendants to produce a Privacy Impact Assessment; only the E-Government Act so mandates, and as concluded above, the Court is not presently empowered to exert judicial review pursuant to the APA with respect to Plaintiff’s claims under the E-Government Act, nor can judicial review be sought pursuant to the E-Government Act itself, since it does not provide for a private cause of action. Consequently, for all of the foregoing reasons, none of Plaintiff’s avenues of potential legal redress appear

to be viable at the present time, and Plaintiff has not demonstrated a likelihood of success on the merits.

C. Irreparable Harm, Balance of the Equities, and the Public Interest

Given that Plaintiff is essentially limited to pursuing an informational injury, many of its theories of irreparable harm, predicated as they are on injuries to the private interests of its advisory board members, have been rendered moot. *See* Pl.’s Am. Mem., at 34–40. Nonetheless, the non-disclosure of information to which a plaintiff is entitled, under certain circumstances itself constitutes an irreparable harm; specifically, where the information is highly relevant to an ongoing and highly public matter. *See, e.g., Elec. Privacy Info. Ctr. v. Dep’t of Justice*, 416 F. Supp. 2d 30, 41 (D.D.C. 2006) (“EPIC will also be precluded, absent a preliminary injunction, from obtaining in a timely fashion information vital to the current and ongoing debate surrounding the legality of the Administration’s warrantless surveillance program”); *see also Washington Post v. Dep’t of Homeland Sec.*, 459 F. Supp. 2d 61, 75 (D.D.C. 2006) (“Because the urgency with which the plaintiff makes its FOIA request is predicated on a matter of current national debate, due to the impending election, a likelihood for irreparable harm exists if the plaintiff’s FOIA request does not receive expedited treatment.”). Indeed, the D.C. Circuit has held that “stale information is of little value . . . [.]” *Payne Enters, Inc. v. United States*, 837 F.2d 486, 494 (D.C. Cir. 1988), and that the harm in delaying disclosure is not necessarily redressed even if the information is provided at some later date, *see Byrd v. EPA*, 174 F.3d 239, 244 (D.C. Cir. 1999) (“Byrd’s injury, however, resulted from EPA’s failure to furnish him with the documents until long after they would have been of any use to him.”). Here, however, the Court concludes that Plaintiff is not presently entitled to the information that it seeks, and accordingly, Plaintiff

cannot show that it has suffered an irreparable informational injury. To hold otherwise would mean that whenever a statute provides for potential disclosure, a party claiming entitlement to that information in the midst of a substantial public debate would be entitled to a finding of irreparable informational injury, which cannot be so. *See, e.g., Elec. Privacy Info. Ctr. v. Dep't of Justice*, 15 F. Supp. 3d 32, 45 (D.D.C. 2014) (“surely EPIC’s own subjective view of what qualifies as ‘timely’ processing is not, and cannot be, the standard that governs this Court’s evaluation of irreparable harm”).

Finally, the equitable and public interest factors are in equipoise. As the Court recently held in a related matter, “[p]lainly, as an equitable and public interest matter, more disclosure, more promptly, is better than less disclosure, less promptly. But this must be balanced against the interest of advisory committees to engage in their work” *Lawyers’ Comm. for Civil Rights Under Law v. Presidential Advisory Comm’n on Election Integrity*, No. CV 17-1354 (CKK), 2017 WL 3028832, at *10 (D.D.C. July 18, 2017). Here, the disclosure of a Privacy Impact Assessment may very well be in the equitable and public interest, but creating a right to such disclosure out of whole cloth, and thereby imposing an informational burden on the Commission where none has been mandated by Congress or any other source of law, is not.

IV. CONCLUSION

For all of the foregoing reasons, Plaintiff’s [35] Motion for a Temporary Restraining Order and Preliminary Injunction is **DENIED WITHOUT PREJUDICE**.

An appropriate Order accompanies this Memorandum Opinion.

/s/

COLLEEN KOLLAR-KOTELLY
United States District Judge

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.

Civil Action No. 1:17-cv-1320 (CKK)

DECLARATION OF KRIS W. KOBACH

I, Kris W. Kobach, declare as follows:

1. I am the Secretary of State of Kansas, having served in that position since 2011. I am also the Vice-Chair of the Presidential Advisory Commission on Election Integrity (the “Commission”), which the President established on May 11, 2017, pursuant to Executive Order 13799. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine Americans’ confidence in the integrity of the federal election process.

2. The information provided in this declaration is based on my personal knowledge and upon information provided to me in my official capacity as Vice-Chair of the Commission.

3. The Commission was established within the Executive Office of the President and is chaired by the Vice President. The membership, not more than fifteen, is appointed by the President. The members of the Commission come from federal, state, and local jurisdictions

across the political spectrum. The Commission, which is solely advisory, is charged with submitting a report to the President containing its findings and recommendations. The duties of the Commission are set forth in Executive Order 13799 (attached as Exhibit 1) and the Commission's Charter (attached as Exhibit 2). Pursuant to the Charter, the records of the Commission and any subcommittees shall be maintained pursuant to the Presidential Records Act of 1978.

4. In furtherance of the Commission's mandate, I directed that identical letters (with different addressees) be sent to the secretaries of state or chief election officers of each of the fifty states and the District of Columbia. The letters solicit the views and recommendations of the secretaries of state and request their assistance in providing to the Commission publicly-available voter roll data to enable the Commission to fully analyze vulnerabilities and issues related to voter registration and voting. Specifically, I asked for the following data, "if publicly available under the laws of your state": full first and last names of registrants; middle names or initials if available; addresses; dates of birth; political party (if recorded); last four digits of social security numbers; voter history (elections voted in) from 2006; active/inactive status; cancelled status; information regarding prior felony convictions; information regarding voter registration in another state; military status; and overseas citizen information. The information requested is similar to the information that states are required to maintain and to make available for public inspection under the National Voter Registration Act (NVRA) and the Help America Vote Act (HAVA). *See, e.g.*, 52 U.S.C. §§ 20507(i), 21083. The letter I sent to the Secretary of State of Alabama, which is representative of all the letters, is attached as Exhibit 3.

5. In these letters, I requested that the states respond by July 14, 2017, and described two methods for responding. I intended that narrative responses, not containing voter roll data,

be sent via email to the address provided in the letter. This email is a White House email address (in the Office of the Vice President) and subject to the security protecting all White House communications and networks. For voter roll data, I intended that the states use the Safe Access File Exchange (“SAFE”), which is a secure method of transferring large files up to two gigabytes (GB) in size. SAFE is a tested and reliable method of secure file transfer used routinely by the military for large, unclassified data sets. It also supports encryption by individual users. My letters state that “documents” submitted to the Commission will be made available to the public. That refers only to the narrative responses. With respect to voter roll data, the Commission intends to de-identify any such data prior to any public release of documents. In other words, the voter rolls themselves will not be released to the public by the Commission. The Commission intends to maintain the data on the White House computer system.

6. To my knowledge, as of July 5, 2017, no Secretary of State had yet provided to the Commission any of the information requested in my letter. I have read media reports that numerous states have indicated that they will decline to provide all or some portion of the information, in some cases because individual state law prohibits such transfer of information. However, it is my belief that there are inaccuracies in those media reports with respect to various states.

7. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 5th day of July 2017.

A handwritten signature in black ink that reads "Kris Kobach". The signature is written in a cursive style with a large, stylized "K" and "C".

Kris W. Kobach

EXHIBIT 1

Federal Register

Presidential Documents

Vol. 82, No. 93

Tuesday, May 16, 2017

Title 3—

Executive Order 13799 of May 11, 2017

The President

Establishment of Presidential Advisory Commission on Election Integrity

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

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

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

Sec. 3. *Mission.* The Commission shall, consistent with applicable law, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President that identifies the following:

(a) those laws, rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections;

(b) those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of the voting processes used in Federal elections; and

(c) those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting.

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

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

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

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

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

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

JA000055

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

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

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

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

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

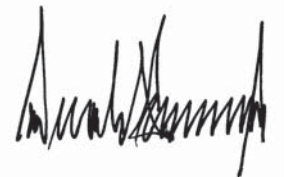
(e) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

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

(g) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

A handwritten signature in black ink, appearing to be the signature of Donald Trump, located at the bottom right of the page.

THE WHITE HOUSE,
May 11, 2017.

EXHIBIT 2

CHARTER

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY

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

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

9. **Estimated Number and Frequency of Meetings.** Meetings shall occur as frequently as needed, called, and approved by the DFO. It is estimated the Commission will meet five times at a frequency of approximately 30-60 days between meetings, subject to members' schedules and other considerations.
10. **Duration and Termination.** The Commission shall terminate no more than two (2) years from the date of the Executive Order establishing the Commission, unless extended by the President, or thirty (30) days after it presents its final report to the President, whichever occurs first.
11. **Membership and Designation.**
 - (a) The Vice President shall chair the Commission, which shall be composed of not more than fifteen (15) additional members.
 - (b) Members shall be appointed by the President of the United States and shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience determined by the President to be of value to the Commission. Members of the Commission may include both regular Government Employees and Special Government Employees.
 - (c) The Vice President may select a Vice Chair from among those members appointed by the President, who may perform the duties of the chair if so directed by the Vice President. The Vice President may also select an executive director and any additional staff he determines necessary to support the Commission.
 - (d) Members of the Commission will serve without additional compensation. Travel expenses will be allowed, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5701-5707), consistent with the availability of funds.
12. **Subcommittees.** The Chair of the Commission, in consultation with the DFO, is authorized to create subcommittees as necessary to support the Commission's work. Subcommittees may not incur costs or expenses without prior written approval of the Chair or the Chair's designee and the DFO. Subcommittees must report directly to the Commission, and must not provide advice or work products directly to the President, or any other official or agency.
13. **Recordkeeping.** The records of the Commission and any subcommittees shall be maintained pursuant to the Presidential Records Act of 1978 and FACA.
14. **Filing Date.** The filing date of this charter is June 23, 2017.

EXHIBIT 3

JA000060



Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable John Merrill
Secretary of State
PO Box 5616
Montgomery, AL 36103-5616

Dear Secretary Merrill,

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

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

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

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

JA000061

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

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

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

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

Sincerely,

A handwritten signature in black ink that reads "Kris Kobach". The signature is written in a cursive, slightly slanted style.

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

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.

Civil Action No. 1:17-cv-1320 (CKK)

SECOND DECLARATION OF KRIS W. KOBACH

I, Kris W. Kobach, declare as follows:

As described in my declaration of July 5, 2017, I am the Vice Chair of the Presidential Advisory Commission on Election Integrity. I submit this second declaration in response to the Court's order of July 5, 2017, requesting answers to five enumerated questions. I have addressed each question below. The answers are based on my personal knowledge and upon information provided to me in my official capacity as Vice Chair of the Commission.

1. Who are the current members of the Presidential Advisory Commission on Election Integrity, and what are their affiliations?

- Vice President Mike Pence, Vice President of the United States, *Chair* (R)
- Secretary Kris Kobach, Secretary of State for Kansas, *Vice Chair* (R)
- Secretary Connie Lawson, Secretary of State of Indiana (R)
- Secretary Bill Gardner, Secretary of State of New Hampshire (D)
- Secretary Matt Dunlap, Secretary of State of Maine (D)
- Ken Blackwell, former Secretary of State of Ohio (R)
- Commissioner Christy McCormick, Election Assistance Commission (R)
- David Dunn, former Arkansas State Representative (D)
- Mark Rhodes, Wood County, West Virginia Clerk (D)
- Hans von Spakovsky, Senior Legal Fellow, Heritage Foundation (R)

- 2. If there are no current members who are officials of a federal agency, what is the likelihood that an official of a federal agency will become a member of the Presidential Advisory Commission on Election Integrity in the near future? Identify any likely members who are currently officials of a federal agency.**

Christy McCormick is a member of the Election Assistance Commission (EAC).

However, Ms. McCormick is not serving in her official capacity as a member of the EAC; she was selected based upon her experience in election law and administration, including as an employee of the U.S. Department of Justice. The Commission has no legal relationship with the EAC. The President has discretion to appoint additional members to the Commission. To my knowledge, however, no other federal agency officials are currently under consideration for appointment to the Commission.

- 3. To what extent has or will the General Services Administration be involved in the collection and storage of data for the Presidential Advisory Commission on Election Integrity?**

At this time, there are no plans for the General Services Administration to collect or store any voter registration or other elections-related data for the Commission.

- 4. Who is the current operator of the website <https://safe.amrdec.army.mil/safe/Welcome.aspx>?**

The U.S. Army Aviation and Missile Research Development and Engineering Center operates that website, which the White House uses for data transfers. *See* <https://safe.amrdec.army.mil/safe/About.aspx>.


- 5. Who is responsible for collecting and storing data received via the website <https://safe.amrdec.army.mil/safe/Welcome.aspx>? Who will transfer that data to the Presidential Advisory Commission on Election Integrity?**

The Safe Access File Exchange (SAFE) is an application for securely exchanging files.

States will upload data to the SAFE website, and Commission staff will download the files from SAFE onto White House computers. As this is a Presidential advisory commission, the White House is responsible for collecting and storing data for the Commission. The Commission's Designated Federal Officer (an employee within the Office of the Vice President) will work with White House Information Technology staff to facilitate collection and storage.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 6th day of July 2017.

A handwritten signature in black ink that reads "Kris Kobach". The signature is written in a cursive, slightly slanted style.

Kris W. Kobach

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

vs.

1:17-cv-1320

PRESIDENTIAL ADVISORY COMMISSION
ON ELECTION INTEGRITY; MICHAEL PENCE,
in his official capacity as Chair of
the Presidential Advisory Commission
on Election Integrity; KRIS KOBACH,
in his official capacity as Vice
Chair of the Presidential Advisory
Commission on Election Integrity;
EXECUTIVE OFFICE OF THE PRESIDENT
OF THE UNITED STATES; OFFICE OF THE
VICE PRESIDENT OF THE UNITED STATES,

Defendants.

TRANSCRIPT OF TEMPORARY RESTRAINING ORDER
BEFORE THE HONORABLE COLLEEN KOLLAR-KOTELLY
UNITED STATES DISTRICT JUDGE

JULY 7, 2017

Court Reporter:
Richard D. Ehrlich, RMR, CRR
Official Court Reporter
United States District Court
333 Constitution Avenue, NW
Washington, DC 20001
(202) 354-3269

Proceedings reported by stenotype.

Transcript produced by computer-aided transcription.

A P P E A R A N C E S

FOR THE PLAINTIFF:

MARC ROTENBERG
ALAN J. BUTLER
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org
butler@epic.org

FOR THE DEFENDANTS:

ELIZABETH J. SHAPIRO
CAROL FEDERIGHI
JOSEPH E. BORSON
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514-5302
Elizabeth.Shapiro@usdoj.gov
Carol.Federighi@usdoj.gov
Joseph.Borson@usdoj.gov

1 THE COURT: Good afternoon, everyone.

2 All right. Go ahead and call.

3 THE CLERK: Civil Case 17-1320, *Electronic*
4 *Privacy Information Center vs. Presidential*
5 *Advisory Commission On Election Integrity, et*
6 *al.*

7 Counsel, would you please come forward and
8 identify yourself for the record?

9 MR. ROTENBERG: Your Honor, good afternoon.
10 My name is Marc Rotenberg. I am counsel for the
11 Electronic Privacy Information Center. With me
12 is Alan Butler, also counsel for EPIC.

13 THE COURT: All right. Good afternoon.

14 MS. SHAPIRO: Good afternoon, Your Honor.
15 I'm Elizabeth Shapiro from the Department of
16 Justice, and with me at counsel's table is
17 Joseph Borson and Carol Federighi, also from the
18 Department of Justice.

19 THE COURT: All right. Thank you.

20 All right. I reviewed the motion for the
21 temporary restraining order, the opposition, or
22 reply, a sur-reply, and a very recently sur
23 sur-reply that I just received.

24 So I have to say that the last document
25 I've received I've looked at very quickly but

1 have not been able to look at everything, but I
2 did look at some of the exhibits, et cetera.

3 So, obviously, I will need to take a look
4 at that a little bit more. I've also reviewed
5 the pertinent case law.

6 I'm going to start by stating my overview
7 of what I consider a framework in very summary
8 forms what I would consider in informing my
9 decision when I make it. I will tell you I'm
10 not making it from the bench today. I do need
11 some information, and that's part of the reason
12 for the hearing.

13 So I'm going to start with the standing
14 arguments as I understand them in looking at the
15 case law. I'm going to start with informational
16 standing or injury and the general principles
17 that you start by looking at the statute that's
18 at issue that requires a disclosure of
19 information. It would appear from the cases
20 that there would be no informational standing if
21 the statute has a prerequisite to the disclosure
22 of the information. That has not yet happened.
23 There would be no informational injury because
24 the Government has not yet been obligated to
25 disclose the information; however, if you

1 consider the E-Government Act, which is the
2 statute at issue in this case, it requires that
3 there be a Privacy Impact Assessment and
4 disclosure of that assessment before the, in
5 this case, the election data is collected. So
6 it would appear that it could apply in this
7 particular case.

8 The Commission moved forward in collecting
9 the electronic -- the election data, rather,
10 where the statute requires an impact statement
11 regarding the collection, and it requires also a
12 disclosure of that impact statement before the
13 collection of the data.

14 So I think this case fits more into that
15 category when you look at the E-Government Act
16 itself which requires all of this before you
17 start collecting.

18 So we're talking about -- in this there's
19 been no impact statement done or disclosed prior
20 to collecting the data at issue, which the
21 E-Government Act requires, and the injury here
22 would be the nondisclosure of the impact
23 statement prior to collecting the election data.

24 In terms of organizational standing, there
25 are at least two theories at issue. One is that

1 the -- which the plaintiff argues that their
2 members are injured or will be injured if the
3 privacy impact statement is not done. It's not
4 clear to me what harm there would be to the
5 individual members, what they would suffer where
6 the Commission is collecting, according to them,
7 only publicly available information and would
8 only publish in an anonymous form. So I need
9 more information relating to the membership and
10 harm.

11 Looking at another theory, which is in the
12 PETA case, which is a DC circuit case, the DC
13 circuit recognized a somewhat unique concept of
14 organizational standing; namely, that an
15 organization has standing if it can show, quote,
16 "A concrete and demonstrable injury to its
17 activities mindful that under our precedent a
18 mere setback to abstract social interest is not
19 sufficient."

20 This would mean that EPIC has standing if
21 it can show that its public interest
22 activities -- I'm assuming educating the public
23 regarding privacy -- will be injured by the
24 defendants' failing to abide by the E-Government
25 Act.

1 So the injury here, it's argued, would be
2 its public interest activities, educating the
3 public, or whatever, and they would not have the
4 information from the Privacy Impact Assessment
5 prior to the collection of the electronic data.

6 So the failure would be to provide EPIC
7 important information that they argue vital to
8 its public interest activities. I need more
9 information about this one as well.

10 So those are, in very summary forms, what I
11 see as the arguments and the framework on which
12 to make a decision on obviously the initial
13 decision which is going to be standing.

14 Now, I have a series of questions that I'd
15 like to ask, and at the end of all of the
16 questions, I'll give you an opportunity to
17 respond to my overview, to my two views of the
18 informational injury and the organizational.

19 So I'm going to start with the plaintiff.
20 So why don't you come on up and let me ask a
21 couple of questions here.

22 So I'm going to start with the members.
23 What concrete harms will EPIC members suffer if
24 their publicly available voter information is
25 collected and publicized by defendants in an

1 anonymous form?

2 MR. ROTENBERG: Okay. Thank you, Your
3 Honor. Let me begin by saying that EPIC will
4 take the position that, as a matter of law, none
5 of the information sought by the Commission is,
6 in fact, publicly available to the Commission.
7 I will explain that I believe it is one of the
8 questions you set out in your hearing for today.

9 The information that is sought from the
10 EPIC members is information that is currently
11 protected under state privacy law. Those state
12 privacy laws limit the collection and use of
13 state voter record information to particular
14 parties and for particular purposes. In our
15 view, the Commission falls outside the bounds of
16 almost all of those exceptions found in the
17 state privacy law for the release of the
18 information that the Commission seeks. That's
19 the basis upon which we say that there is
20 nothing as a matter of law that's publicly
21 available to the Commission given the request in
22 the June 28th letter.

23 THE COURT: Well, it seemed to me -- and I
24 only got to look at the chart very quickly as
25 one of the exhibits, but it looked as if a

1 number of states were providing some; a number
2 of states were indicating that they couldn't
3 under their state statutes. There may be some
4 federal statutes relating to Social Security.
5 The Commission has argued that it's only
6 publicly available that they're seeking, and if
7 a state has statutes that would not allow it to
8 produce it, then they are not expecting to get
9 the information.

10 MR. ROTENBERG: Right. We understand that,
11 Your Honor, and we've attached by way of example
12 the response from the Secretary of State of the
13 State of Georgia, which was similar to the
14 responses from many of the states in which the
15 state secretary says simply much of the
16 information that is sought by the Commission we
17 could not release.

18 But then you see the state secretary goes
19 on to suggest that there are additional
20 conditions prior to the disclosure. So, for
21 example, the method that has been proposed by
22 the Commission to receive the voter data from
23 the State of Georgia, even that could be
24 permissibly disclosed by the State, the State
25 would not accept, and the State said we would

1 have to find a different technique, one that is
2 password encrypted and authenticated to permit
3 the release of the personal data; moreover, the
4 State of Georgia also said to the Commission
5 there are fees associated when requests are made
6 for the release of state voter data.

7 The June 28th letter that was sent to the
8 50 state secretaries provided no indication that
9 the Commission was prepared to pay any of the
10 fees associated with a release of the data it
11 was seeking.

12 So you see, there are three different ways
13 to understand how it is that when the Commission
14 approaches the State and asks for so-called
15 publicly available information, the state
16 secretary properly responds under the terms of
17 this letter, "There's, in fact, nothing we can
18 provide to you."

19 THE COURT: So your idea would be that if
20 they had done an impact -- Privacy Impact
21 Assessment, they would've figured this all out?

22 MR. ROTENBERG: Well, Your Honor, that's
23 the second category of our objection to the
24 Commission's request. Not only do we believe
25 that the states could not release the

1 information to the Commission, we further
2 believe that the Commission could not receive
3 the information from the states, and this has to
4 do with the obligations that fall on the
5 Commission by virtue of being within the
6 Executive Office of the President and subject to
7 the Federal Advisory Committee Act and the
8 E-Government Act to undertake certain steps
9 before it could request any type of personal
10 data. It was expected to undertake the Privacy
11 Impact Assessment, which may very well have
12 revealed that the method of transmission
13 proposed in this instance was simply inadequate.

14 So you see, in requesting the so-called
15 publicly available information, the Commission
16 actually committed two flaws. In the first
17 instance, it did not comply with the requests of
18 the 50 states.

19 In the second instance, it did not fulfill
20 its own obligations to safeguard the information
21 it was intending to collect.

22 THE COURT: Okay. But let's get -- that
23 one gets a little bit more to the merits it
24 seems to me.

25 MR. ROTENBERG: Yes.

1 THE COURT: Let me get back to sort of the
2 standing question. I appreciate the
3 information.

4 What concrete harms -- I'm talking about
5 this is -- the EPIC members would suffer if --
6 assuming that there is any publicly available
7 voter information that can actually be
8 collected. I believe that they've indicated --
9 I mean, if they're not publicly available,
10 they're not going to receive it, and you've
11 indicated that -- I don't know whether anybody
12 has actually sent anything or whether any of the
13 states can say that they can send it. They're
14 meeting all of the requirements. Do you know?

15 MR. ROTENBERG: Well, let me say based on
16 the declaration of Mr. Kobach on July 5th, two
17 days ago, the Commission had not received any
18 data from any of the states.

19 So, at this moment, we're relying on that
20 declaration as to the current status regarding
21 the transfer of the data that's being sought.

22 But to your question, Your Honor, let's
23 understand two different types of information
24 that the State is seeking. So by the terms of
25 the letter, they ask, for example, for the last

1 four digits of the Social Security number.
2 Members of EPIC's voter information may well
3 contain the Social Security number. It is often
4 used in the state administration of election
5 systems to avoid duplication and reduce the risk
6 of fraud, but it is not the case that
7 information is generally made available to the
8 public. If it were made available to the
9 public, the last four digits of the Social
10 Security number have been identified by the
11 Department of Justice and consumer protection
12 agencies as contributing to the commission of
13 identity theft and financial fraud because those
14 last four digits are the default passwords for
15 many commercial services such as cell phone or
16 online banking.

17 So you see, the Commission has asked the
18 states to turn over particular personal
19 information the states would not routinely make
20 available concerning EPIC members that if it
21 were made public could lead to identity theft.

22 THE COURT: But that assumes -- I think
23 they've indicated, however, that publicly
24 available -- they've left it to the states to
25 figure out, or whatever statutes. So if there's

1 a federal statute or some other way that they
2 should not be giving out Social Security
3 numbers, or the last four digits of Social
4 Security numbers, the expectation would be that
5 the states would not provide it.

6 MR. ROTENBERG: I understand your point,
7 Your Honor, but I would add also, I frankly find
8 it striking that a commission on election
9 integrity would make such a broad request to the
10 states for such detailed personal information
11 and then put it back on the states to determine
12 which information the states may lawfully
13 release.

14 Let me take a simple category. Home
15 addresses. So there is agreement, for example,
16 in the report of the National Conference of
17 State Legislatures, the 2016 report which we've
18 appended to our filing, that surveys the privacy
19 laws of all 50 states. And it says, 29 states,
20 as a general matter, will give out home
21 address -- name and address, I should say
22 precisely, name and address information.

23 And you could well say, "Well, that appears
24 to be publicly available information. Why can't
25 they just, you know, send back the name and

1 address information?"

2 And then you read more closely, and you see
3 that, in fact, even though that information may
4 be made available, many people in the states
5 also have the right to restrict the disclosure
6 of name and address information.

7 Texas, in fact, restricts the disclosure of
8 the name and address information from the
9 judiciary.

10 So none of these categories lend themselves
11 to an easy release of state data.

12 THE COURT: Well, it sounds as if there's
13 not going to be any basis for them to get
14 anything. So your request to hold it back, if
15 they're not going to give it, doesn't seem to
16 work.

17 I'm still trying to get in terms -- what
18 are the EPIC -- let me ask it this way: Who do
19 you consider the EPIC members? Their advisory
20 board. What does the advisory board do? I
21 mean, the members that you're talking about, the
22 ones you attached were advisory board members
23 and also voters. So what are the rights and
24 responsibilities of EPIC's advisory board
25 members?

1 MR. ROTENBERG: Okay. So we have
2 approximately 100 members of our advisory board.
3 They are leading experts in law, technology, and
4 public policy that contribute to the support of
5 the organization. They participate in the work
6 of the organization. They help select award
7 recipients for the organization.

8 THE COURT: Do they pay any kind of dues?

9 MR. ROTENBERG: There is no formal dues
10 requirement, but most of the members do
11 contribute in some manner to the work of the
12 organization. And in this particular matter, 30
13 of our 100 members signed a statement to the
14 National Association of Secretaries of State
15 asking state officials not to release the voter
16 data to the Commission.

17 So we are, in effect, also representing
18 their interest when we appear before --

19 THE COURT: Who is their interest?

20 MR. ROTENBERG: I'm sorry?

21 THE COURT: Who is their interest?

22 MR. ROTENBERG: Those members of our
23 advisory board who are actively participating
24 and expressing their opposition to the data
25 collection.

1 THE COURT: Okay. Do they control the
2 activities of the organization?

3 MR. ROTENBERG: They do not directly
4 control the activities of the organization.
5 There is a separate board of directors, but it
6 is not uncommon for an organization such as EPIC
7 to have this structure, and the members of the
8 advisory board actively participate in the
9 program activities and the direction and
10 selection of matters that the organization
11 pursues.

12 THE COURT: So exactly what -- the board of
13 directors runs the organization?

14 MR. ROTENBERG: Yes, that's correct.

15 THE COURT: And the advisory board advises
16 on what matters to get involved with?

17 MR. ROTENBERG: Yes, Your Honor, and
18 actively participates in those activities and
19 provides financial support.

20 THE COURT: But it's a voluntary financial
21 support?

22 MR. ROTENBERG: That's correct. But they
23 could not -- to be clear on this point, they
24 could not be a member of the advisory board
25 unless they formally accepted that

1 responsibility, and they may choose to withdraw
2 their participation as an advisory board member
3 as well.

4 THE COURT: Accepted what responsibility?

5 MR. ROTENBERG: Participating in the work
6 of the organization.

7 THE COURT: Okay.

8 MR. ROTENBERG: Contributing to its
9 activities.

10 THE COURT: And the contribution you're
11 talking about is contributing in terms of if you
12 decide to take on a particular task such as this
13 one, this particular case, that they would
14 contribute to providing information, pursuing
15 it? Is that what you're saying?

16 MR. ROTENBERG: Financial support including
17 personal donations are routinely made by members
18 of the advisory board, their time and their
19 expertise.

20 THE COURT: All right. So what
21 informational harms will EPIC suffer if the
22 defendants don't comply with the E-Government
23 Act, which requires disclosure of this Privacy
24 Impact Assessment to be done and then disclosed
25 before the collection of the data?

1 Again, I'm talking about EPIC in the
2 context of either membership or otherwise.

3 MR. ROTENBERG: Right. Well, apart from
4 the individual harm to our members, also as an
5 organization that was specifically established
6 to focus public attention on emerging privacy
7 issues, and has been involved in the voter
8 privacy matter for almost 20 years, this
9 particular controversy directly impacts our
10 mission. This is not a speculative type of
11 arrangement. This is a circumstance where we
12 have for many years sought to advance an
13 interest in voter privacy here in the United
14 States. The actions by the Commission have
15 required us to undertake a number of activities
16 to work with citizen organizations, to discuss
17 with media outlets the impact of the
18 Commission's activity upon the public. That is
19 an educational function which we would not be
20 doing at this point to the extent that we are
21 but for the Commission's request to gather state
22 voter record information.

23 THE COURT: So as you've described it, I
24 take it that's what you would consider your
25 public interest activities?

1 MR. ROTENBERG: Well, yes. I mean, there
2 is, in fact, also related litigation. We are
3 seeking under the Open Government Act to obtain
4 information about the Commission's activity.
5 That is also activity undertaken, a cost to the
6 organization, and in response to the
7 Commission's act.

8 THE COURT: All right. And in terms of
9 educating the public regarding data privacy or
10 other activities, do you use routinely
11 information from the Government?

12 MR. ROTENBERG: Yes, we do, and I should
13 point out also central to our educational
14 activity is the maintenance of one of the most
15 popular websites in the world on privacy issues,
16 which is simply EPIC.org. So for the last week,
17 as a consequence of the Commission's act, we put
18 aside the other work on our website and focused
19 solely on providing public information related
20 to this current controversy.

21 So there are two pages of EPIC.org with
22 extensive information about the Commission as
23 well as this litigation.

24 THE COURT: You started off the discussion
25 by indicating all of the difficulties and

1 barriers there would be to provide -- having the
2 states provide the voter registration data to
3 the Commission based on various statutes,
4 regulations, or whatever. I take it you're
5 really getting to the merits that this is not
6 publicly available for the most part? Is that
7 the point of this --

8 MR. ROTENBERG: Correct, Your Honor. And
9 we thought it was important to state that at the
10 outset. We understood in the questions that you
11 had posed to the parties for today's hearing,
12 and certainly Mr. Kobach in his letter to the
13 state secretaries, uses this phrase, "publicly
14 available." He places a great deal of weight on
15 it. But, in fact, we could not find the phrase
16 in any of the state voter privacy laws that we
17 looked at. The states talk about public records
18 in some instances, or they talk about exemptions
19 which permit the release of voter record
20 information. But we thought it was very
21 important to make clear that this phrase is
22 actually not a phrase that helps us understand
23 the permissible circumstances under which the
24 data may be released.

25 THE COURT: Okay. All right. I have some

1 questions for the defendant. I'll get back to
2 you.

3 MR. ROTENBERG: Okay. Thank you.

4 THE COURT: So my first question is:
5 What's the authority, if any, relied on by the
6 Commission to systematically collect this voter
7 registration information?

8 I didn't see anything in the materials
9 establishing or anything else that talked about
10 it.

11 MS. SHAPIRO: Well, I think the main
12 authority is the executive order which sets out
13 the mission of the Commission and the charter
14 based on the executive order. And in order to
15 carry out the work that is defined in those
16 documents, the Commission needs to collect and
17 analyze information so that it can best advise
18 the president in the report that it's charged
19 with creating.

20 THE COURT: But you would agree that
21 there's nothing in the executive order that
22 suggests that you -- that this data should be
23 collected?

24 MS. SHAPIRO: There's nothing specific
25 about that, but I don't believe that authority

1 would be required because it's not a demand for
2 information. It's a request, and the Commission
3 is not empowered to enforce that. It doesn't
4 have the ability to say you must do it. So it's
5 simply a request to the states and nothing more
6 than that.

7 THE COURT: Do you want to respond to the
8 issue in terms of what he brought up initially
9 relating to the fact that, as it appears that
10 most states, if not all of them, have
11 restrictions, and that there's really nothing
12 that's totally publicly available about the
13 request?

14 MS. SHAPIRO: So I think if I'm
15 understanding correctly, I think what EPIC is
16 saying is that they don't have standing because
17 the way I understand what they're saying is that
18 the states are not going to provide the
19 information because the information is protected
20 under state law, in which case there won't be
21 information going to the Commission. So there
22 can't possibly be any injury because if the
23 information is not going to the Commission,
24 there's no injury. There's no Article III
25 standing.

1 THE COURT: Are you talking about in the
2 context of the EPIC injury to EPIC members? Is
3 that what you're talking about?

4 MS. SHAPIRO: EPIC members.

5 I also wanted to address the alleged
6 organizational injury because I think that they
7 fail standing on numerous levels. Not only do
8 the members not have standing because their
9 states are not providing the information, but,
10 organizationally, everything that EPIC just
11 discussed now relates to its advocacy mission.
12 And I think the cases are quite clear that
13 simply choosing where to allocate resources when
14 advocating --

15 THE COURT: But that's only one piece of
16 what he talked about. I mean, if you look at
17 the PETA case, it certainly is -- the argument
18 would be its public interest activities, which
19 in this case is educating the public is that by
20 not having the information relating to the
21 assessment, the impact assessment, they're not
22 in a position to put that information out.

23 So, I mean -- leaving aside allocating
24 different things. The questions I asked really
25 related to what was the role of the members in

1 order to make a decision as to whether, you
2 know, the first theory of organizational
3 standing based on membership as opposed to the
4 PETA case, which I think is premised on
5 activities, not on membership.

6 MS. SHAPIRO: Correct. Though the PETA
7 case identified a concrete injury to the
8 organization, a perceptible injury they called
9 it, because they were not -- in that case, there
10 was agency -- some agency inaction that
11 prevented the organization from filing
12 complaints with the agency. So there was a
13 perceptible injury to the organization.

14 Here you have an organization whose mission
15 is advocacy. They may be very, very interested
16 in privacy, and they may be expert --

17 THE COURT: Advocacy but also in terms of
18 informing the public, if I understood. The
19 educational aspect would be informing the public
20 of this information, and they're not getting it.

21 MS. SHAPIRO: Correct, but the information
22 doesn't exist, and I guess that goes to the
23 informational standing because I believe that
24 the cases require that the information actually
25 be in existence in order to --

1 THE COURT: You have to look at the statute
2 first. And if you look at the statute, the
3 E-Government Act requires that before the
4 collection of the data take place, that you
5 would've done this impact statement, which is
6 different than the cases that have indicated
7 where the statute requires. What I said is that
8 the prerequisite to the disclosure hadn't
9 happened in the other case, which I think is --
10 I can't remember which case it is.

11 MS. SHAPIRO: It was Friends of Animals, I
12 think.

13 THE COURT: Yeah, in terms of that one,
14 which is not what we're talking about.

15 E-Government Act doesn't require -- it
16 requires it up front before you would've
17 collected data.

18 MS. SHAPIRO: Yes. But I think, then, it's
19 a question of the Commission not being subject
20 to the E-Government. So it has no requirement
21 to create that --

22 THE COURT: That's why we're getting back
23 to some of these standing things.

24 MS. SHAPIRO: Right.

25 THE COURT: So let's get back to some of

1 the other questions that I had.

2 So your view of it is it's implicit in the
3 executive order that they can collect whatever
4 they think is important for their mission?

5 MS. SHAPIRO: Right. And I would refer
6 back to the Mayer case, which was the Reagan
7 Task Force on Deregulation that was addressed in
8 *Mayer v. Bush*, a similar kind of commission
9 chaired by the vice president also gathering
10 information in order to make recommendations.

11 It's not uncommon to think that in the
12 ordinary task of preparing a report and studying
13 an issue, that you would need information.

14 THE COURT: Okay. I just was curious as to
15 whether there was something I had missed.

16 What services have or will be provided by
17 GSA to the Commission? Because I notice that
18 the executive order says that, "GSA shall
19 provide the Commission with administrative
20 services, funds, facilities, staff, equipment,
21 other support services as be necessary."

22 So have they -- is the Commission fully
23 operational? Have they set up an office? Where
24 is it located? Are you using any GSA services?

25 MS. SHAPIRO: So the Commission is in its

1 infancy. There has not yet been a meeting. GSA
2 is tasked with specific limited administrative
3 support, like arranging travel for the members,
4 maybe assistance with booking meeting locations.
5 Mostly logistical. That's what's envisioned at
6 this stage.

7 THE COURT: Okay. Is that what you're
8 expecting it to do in the future?

9 MS. SHAPIRO: Yes. Of course, the
10 Commission is not really up and running, you
11 know, to any great extent.

12 THE COURT: Where is it located at this
13 point? Does it have an office?

14 MS. SHAPIRO: Well, I don't know that it
15 has dedicated office space. I believe it's the
16 Office of the Vice President, since the vice
17 president is the chair of the Committee.

18 THE COURT: All right. What has been or
19 will be the involvement of Commissioner Christy
20 McCormick and/or the Election Assistance
21 Commission in the decision-making process of the
22 Commission since she heads the Election
23 Assistance Commission?

24 MS. SHAPIRO: She's a member of the
25 Commission but not there as part of her EAC

1 role. It's completely distinct from that.
2 She's there as just a member of the Commission
3 due to her expertise, and she would participate
4 in the decision-making and the deliberations to
5 the extent she's present at the meetings.

6 THE COURT: So there's not going to be any
7 role or any information provided or any role by
8 Election Assistance Commission? Is that what
9 you're saying?

10 MS. SHAPIRO: Well, she would not be there
11 as part of -- in her capacity -- in that
12 capacity as --

13 THE COURT: Well, that's not quite what I
14 asked.

15 MS. SHAPIRO: Okay.

16 THE COURT: What I asked is -- she's maybe
17 not as the head assigned to it like the state
18 secretary of a particular state, but my question
19 is whether the Election Assistance Commission is
20 going to provide assistance to the Commission?

21 So you have her -- I mean, there's cases
22 that talk about dual role of being in sort of a
23 private in the government.

24 MS. SHAPIRO: Right. I'm not aware that
25 they would be providing any assistance. I can

1 double-check that for the Court, but my
2 understanding is that they would not be
3 providing assistance, and she is on the board
4 simply as a member of the Commission.

5 THE COURT: All right. The executive order
6 talks about other federal agencies will, quote,
7 "Cooperate with the Commission."

8 Any other federal agencies currently
9 cooperating with the Commission?

10 MS. SHAPIRO: No. Right now there are no
11 other federal members of the Commission. I
12 don't know of any other federal agencies working
13 with the Commission.

14 THE COURT: So let me move into the website
15 in terms of which -- it appears to be an Army
16 website?

17 MS. SHAPIRO: Yes.

18 THE COURT: So that's not going to be --
19 that doesn't involve a federal agency?

20 MS. SHAPIRO: Well, it's a site that exists
21 to transfer large data sites, but that is more
22 of an IT tool. It's not -- it doesn't involve
23 their -- the military is not engaged in the work
24 of the Commission in any substantive way.

25 THE COURT: Let me ask it this way. Who

1 operates the website that's named in the
2 Commission's request? Is that a component of --
3 it looks -- they did an impact statement
4 themselves about the website, the DOD did, which
5 is obviously a federal agency, or will be
6 considered under the definition.

7 So who is going to actually operate the
8 website? Somebody has to. I assume it's not
9 the Commission. Is it the DOD?

10 MS. SHAPIRO: So the way I understand it
11 works is that the user uploads the data, and
12 then it's downloaded by the Commission; that DOD
13 doesn't play a role in that other than
14 maintaining the site. They don't store the
15 data. They don't archive the data. It deletes
16 after two weeks I believe is the maximum amount
17 of time.

18 THE COURT: So say this again. They
19 maintain it?

20 MS. SHAPIRO: Well, it's their site.

21 THE COURT: Right. So they receive the
22 data and maintain it for the two weeks?

23 MS. SHAPIRO: Well, the person uploading
24 the data can set the time that --

25 THE COURT: And who is uploading the data?

1 MS. SHAPIRO: The states, for example. If
2 they want to upload the data to the site, they
3 can set an expiration date of -- it must be less
4 than two weeks. So a maximum of two weeks that
5 it can remain on the server.

6 THE COURT: So DOD, according to you, has
7 no role?

8 MS. SHAPIRO: That's right, other than, of
9 course, that it runs the SAFE system.

10 I did want to address, since we're talking
11 about that system, the declaration that the
12 plaintiff put in about getting insecure or error
13 messages. If you read through the website for
14 SAFE itself, it's clear that it's tested and
15 certified to work with Windows XP and Microsoft
16 Explorer. So the browsers that EPIC's declarant
17 used were Google and Netscape, I believe, not
18 Explorer. If you plug it into Explorer, it
19 works just fine. And that's in two different
20 places on the website where it makes that clear,
21 that that's the browser that you need to use.

22 I have actually compiled some of the
23 pertinent information from the SAFE site that I
24 can provide to the Court and a copy for the
25 plaintiff as well, if it's helpful.

1 THE COURT: Certainly.

2 So let me see if I understand it. The
3 computer system that's going to operate in terms
4 of this information, you seem to be saying that
5 the website by DOD is sort of like a conduit,
6 shall we say --

7 MS. SHAPIRO: Yes.

8 THE COURT: -- to a system of your own.

9 So you're going to have your own database
10 at the Commission?

11 MS. SHAPIRO: So I don't know exactly what
12 the Commission -- it will be stored in the White
13 House email, or the White House servers. So it
14 will be on the White House system. But what the
15 Commission is going to do by way of using the
16 data and compiling the data, I can't speak to
17 that yet.

18 THE COURT: So you're assume it's either
19 going to be the Commission or the White House
20 that would own and operate the computer system
21 on which the data is going to be stored?

22 MS. SHAPIRO: Yes. And the email address
23 that was provided in the letter to the states is
24 a White House email address that's maintained by
25 the White House, the same system that supports

1 the president and the vice president and secures
2 their communications.

3 THE COURT: So it gets on the DOD. Then
4 how is it going to be transferred to the White
5 House computer system? Who is doing that?

6 MS. SHAPIRO: So my understanding is that
7 the Commission then downloads the information
8 from SAFE, and then it would be kept in the
9 White House systems.

10 THE COURT: So they have an IT staff that's
11 expected to do this?

12 MS. SHAPIRO: Well, I don't know how
13 they're using or going to use IT staff, but the
14 Office of Administration, which serves the
15 Office of the President generally is also within
16 the Executive Office of the President and
17 maintains the White House systems.

18 THE COURT: You also -- I believe it was a
19 letter that gave an email address. Who owns and
20 operates the computer system associated with the
21 email?

22 MS. SHAPIRO: So that's the White House --
23 the ovp.gov address.

24 THE COURT: So this will be on the White
25 House --

1 MS. SHAPIRO: Yeah.

2 THE COURT: And so any other agencies,
3 federal agencies provide support services for
4 the White House's computer system?

5 MS. SHAPIRO: Well, I think that's a
6 complicated question simply because some of the
7 details about how the -- the mechanics of the
8 White House IT is something that may not be
9 appropriate to say in a public setting
10 because --

11 THE COURT: Well, let me just put it this
12 way. Obviously, I'm trying to see if you're
13 getting any -- your argument is E-Government Act
14 doesn't apply because there's no federal agency
15 that's involved.

16 MS. SHAPIRO: Yes.

17 THE COURT: So I'm exploring whether there
18 actually is a federal agency that's involved.

19 MS. SHAPIRO: I understand, but I think the
20 test is not necessarily to look to see if
21 there's one member or one little piece of
22 support.

23 THE COURT: No. I'm just trying to see in
24 terms of how the data would be -- would come, be
25 collected, stored, whether you're doing a

1 separate database or how you're doing this. You
2 seem to be indicating that DOD's website would
3 maintain it at least for the period of time
4 until it got transferred, right?

5 MS. SHAPIRO: Yes. This conduit system
6 would have it for -- until it's downloaded. So
7 from the time it's uploaded until the time it's
8 downloaded for a maximum of two weeks and
9 shorter if that's what's set by the states.

10 THE COURT: And then you also talked about
11 at some point, although it would be allegedly
12 anonymous, but what system is going to be used
13 to publish the voter information?

14 MS. SHAPIRO: Well, one publication I think
15 is unclear at this point because it's not clear
16 what would be published. I think Mr. Kobach
17 made clear that the raw data would not be
18 published. That's just -- we don't know at this
19 point.

20 THE COURT: So do you know who would be
21 making it anonymous? Who would be involved in
22 doing this?

23 I guess the other question is: Is the
24 White House server in a position to take -- I
25 mean, this is a lot of information. Assuming

1 all these states actually provided you the
2 information, are they going to actually handle
3 it?

4 MS. SHAPIRO: I assume --

5 THE COURT: I could see DOD handling it,
6 but do you know?

7 MS. SHAPIRO: I don't know, but I'm
8 assuming they have a way to handle it.

9 THE COURT: All right. I guess I'll start
10 with you and then work back to EPIC, but this is
11 sort of your best arguments on irreparable harm.

12 How are the defendants harmed if they're
13 required to conduct and disclose a privacy
14 assessment before collecting voter information?
15 Is there any harm to you to do this before you
16 had collected it?

17 MS. SHAPIRO: Well, yes. I mean,
18 because -- our position is that they're not
19 subject to the E-Government Act because they're
20 not an agency, then we would be required to do
21 something that we're not required to do. So I
22 think there's inherent harm there.

23 And, you know, there's also a certain
24 amount of -- you know, the privacy assessment is
25 normally done by specific officers and agencies.

1 So it's set up in a way that doesn't fit very
2 well to the Commission. It talks about chief
3 information officers and positions that are
4 appointed as part of the E-Government Act in
5 agencies. But because the Commission is not an
6 agency, it doesn't have those things. So there
7 would be a certain amount of figuring out what
8 to do with that.

9 THE COURT: Well, I was provided -- I
10 didn't get a chance to look at all of the
11 exhibits, but it looks as if the Government, or
12 DOD, has already done a -- pursuant to the E-Gov
13 Act -- a privacy impact statement for the
14 website issued by DOD that you plan on having
15 all of this data at least be maintained
16 initially?

17 MS. SHAPIRO: We got the exhibits 30
18 minutes before we came here. So I haven't
19 studied them, but that's what it appears to be.
20 But DOD is an agency but the Commission is not.

21 THE COURT: Okay. And any public interest
22 in foregoing this privacy assessment?

23 MS. SHAPIRO: I'm sorry. Public interest?

24 THE COURT: Any public interest? I mean,
25 it's one of the things you have to weigh.

1 What's your public interest in not doing it?

2 MS. SHAPIRO: Well, I think --

3 THE COURT: This is around doing a privacy
4 assessment.

5 MS. SHAPIRO: I understand.

6 I think initially plaintiff is seeking
7 extraordinary emergency relief. So, really, the
8 burden is on them, but I think --

9 THE COURT: I'm going to ask them the same
10 thing, but I'm just asking you. I mean,
11 balancing public interest, is there anything in
12 your perspective?

13 MS. SHAPIRO: I mean, I think the public
14 interest is that there's, you know, been a
15 priority that there's important work to be done
16 by this commission, and that it should be
17 permitted to go forward, and, you know, do the
18 mission that the president thinks is important
19 to have done. That's in the public interest, to
20 be able to carry on that work.

21 So, you know, I think there's a public
22 interest in proceeding versus we believe no
23 public interest in the contrary because there's
24 no standing and because there's not an agency
25 involved that's required.

1 THE COURT: Then, obviously, I have to find
2 standing before we got to this issue.

3 MS. SHAPIRO: Yes.

4 THE COURT: I just wanted to see what your
5 answer would be.

6 Okay. Thank you.

7 MS. SHAPIRO: I wanted to say one more
8 thing before I forgot.

9 THE COURT: Certainly.

10 MS. SHAPIRO: When Mr. Kobach filed his
11 declaration, his first declaration I think on
12 July 5th, we said that no information had come
13 into the site. But yesterday the State of
14 Arkansas did transmit information, and it has
15 not been downloaded. So it hasn't been
16 accessed, but it is in the SAFE site.

17 THE COURT: So it's on the DOD site?

18 MS. SHAPIRO: Yes.

19 THE COURT: That you called a SAFE site.

20 MS. SHAPIRO: Yes.

21 THE COURT: Okay.

22 MS. SHAPIRO: Would Your Honor want a copy?

23 THE COURT: Yes. If you pass it up to
24 Ms. Patterson, I'd appreciate it, and give it to
25 plaintiffs.

1 MS. SHAPIRO: Your Honor, I have one more
2 handout, if Your Honor wants it, that relates to
3 standing. It's simply a copy of a decision from
4 2014, from Judge Amy Berman Jackson that
5 involves EPIC. It's called *EPIC vs. Department*
6 *of Education*, and it addresses the
7 organizational standing really in very
8 closely analogous circumstances.

9 THE COURT: Yeah. I'm familiar with the
10 case. I know what it is.

11 MS. SHAPIRO: I know you are. Okay.

12 THE COURT: Thank you.

13 But let me just ask one last question.
14 Since DOD is maintaining -- their website is
15 maintaining the data, why shouldn't they do the
16 assessment? They're a federal agency, and
17 they're basically involved in at least
18 maintaining of the data that's being collected.
19 So why shouldn't they, as a federal agency, do
20 an impact statement relating to the data that
21 they have on their website?

22 MS. SHAPIRO: So I understand that they've
23 done an assessment for the site, and it can't --

24 THE COURT: But for the site in general.

25 MS. SHAPIRO: Right. But it can't be the

1 case that when you have a sharing site like
2 this, it acts as a conduit, that every time
3 information is uploaded, that you have to have a
4 separate Privacy Impact Assessment.

5 THE COURT: I don't know that that's
6 necessarily true. I mean, it seems to me --
7 I'll have to go back and look at the E-Gov Act,
8 but it seems to me if you were dealing with
9 issues of data and privacy, certainly election
10 registration data may be different than some
11 other data in terms of what it would -- what
12 would be done, why they wouldn't be obliged to
13 do one.

14 MS. SHAPIRO: Because there are very
15 specific requirements. Even in the E-Government
16 Act, they have to be collecting the information.
17 And I think when they are passive --

18 THE COURT: Well, aren't they collecting
19 it?

20 MS. SHAPIRO: Well, no, because they're a
21 passive website that -- I mean, a passive site
22 that people upload the information to. You
23 know, DOD is not monitoring what information is
24 being uploaded. It is a way to be able to send
25 large data sets.

1 THE COURT: But that's true of anything
2 that they use this website for, but they went
3 ahead and did one.

4 MS. SHAPIRO: They did one for the system.

5 THE COURT: Right. But, obviously, they
6 thought that it was appropriate to do it. I
7 don't understand the distinction.

8 MS. SHAPIRO: So I think the distinction is
9 to do it for the security of the site. Writ
10 large is one thing, but to do it every time a
11 user anywhere in the country happens to upload
12 information into it, I don't think it's either
13 required or would be rational.

14 THE COURT: Well, it may depend on what the
15 information is that's, you know, that's being
16 collected and maintained on the website.

17 MS. SHAPIRO: I don't think DOD would even
18 know that.

19 THE COURT: I mean, it may be that they
20 would say their impact statement says there
21 isn't anything further to be said. It's safe as
22 we said before. But I'm just saying, I don't
23 understand why you wouldn't do it if the
24 information is of this type of nature, the
25 nature of this voting registration information.

1 MS. SHAPIRO: DOD is not monitoring the
2 substance of the information that's coming in.
3 They're not going to know people are uploading
4 different data sets.

5 THE COURT: Well, it does make a
6 difference. The information is going to sit
7 there. Certainly people could potentially have
8 access to it. It could be hacked or whatever
9 else. Why would you not -- why would they not
10 be required to do one?

11 MS. SHAPIRO: I think for the reason that
12 the operation of the system, one doesn't fit
13 within the definition of when they're required
14 to do one because they're not collecting as the
15 passive site, but also the practicality of any
16 time somebody uploads information to that site,
17 be it for a day or for the maximum of two weeks,
18 DOD is not monitoring that. They don't know
19 that. They don't know what's in the data. It's
20 a secure passageway.

21 So the idea --

22 THE COURT: So are you relying on the E-Gov
23 Act to say that they would not need to do it
24 based on their role in this particular case?
25 I'm trying to figure out what you're relying on.

1 MS. SHAPIRO: Well, I think that's part of
2 it, yes. So we haven't -- that issue was not
3 before us, so we haven't fully analyzed the
4 requirements of the E-Government Act as applied
5 to DOD, but it does require some active
6 collection.

7 THE COURT: Okay. All right.

8 MS. SHAPIRO: Thank you.

9 THE COURT: Thank you.

10 MR. ROTENBERG: Your Honor, if I may. I
11 think I have the precise answer to the question
12 you just posed to counsel.

13 THE COURT: All right.

14 MR. ROTENBERG: We attached in our
15 supplementary motion this afternoon Exhibit 5,
16 which is, in fact, the Privacy Impact Assessment
17 for the SAFE system, and the very first question
18 asks regarding who the information will be
19 received from. The first box, which is "yes" --

20 THE COURT: Hold on one second. This is
21 the very last one you put in the file, right?

22 MR. ROTENBERG: Yes. This is the Notice of
23 Filing of Supplemental Exhibits --

24 THE COURT: Okay.

25 MR. ROTENBERG: -- relevant to the

1 questions raised in the Court's order.

2 THE COURT: I'm sorry. And you're looking
3 at -- which exhibit number is it?

4 MR. ROTENBERG: We're looking at Exhibit 5,
5 the very first page.

6 THE COURT: Okay. I see it.

7 MR. ROTENBERG: And do you see, there are
8 different scenarios. In fact, the DOD is very
9 much aware of who makes use of the website. The
10 first option refers to receiving information
11 from members of the general public. That box is
12 not checked. It's the subsequent box which says
13 from federal personnel and/or federal
14 contractors. That box is checked. And state
15 secretaries would not qualify on that basis.

16 Moreover, if I may point out, these are
17 pages 32 and 33 in the ECF, the PIA sets out a
18 fairly narrow set of circumstances under which
19 it may be used for the transfer of official
20 information. And as to the question do
21 individuals have the opportunities to object,
22 the basis of saying "yes" is by not sending
23 personally identifiable information through the
24 transfer system.

25 So we would say by the terms of the

1 agencies' own Privacy Impact Assessment, it is
2 not suitable for the purpose that the Commission
3 proposes.

4 But if I may make one other point that is
5 also relevant to this. We actually don't
6 believe that the Commission had the authority to
7 turn to the military agency to receive the
8 information because if you look at both the
9 executive order and the Commission's charter, it
10 is the GAO that is described as providing not
11 only administrative services but also --

12 THE COURT: GAO or GSA?

13 MR. ROTENBERG: GSA. Thank you.

14 It is the GSA that provides not simply
15 administrative services, this is not just, you
16 know, arranging travel plans, this is also
17 facilities and equipment. Those words appear in
18 the president's executive order. And in the
19 charter implementing the work of the Commission,
20 paragraph 6 describes, quote, "The agency
21 responsible for providing support."

22 And in that paragraph, these terms
23 "administrative services, facilities, and
24 equipment" appear as well.

25 So it's entirely unclear to us upon what

1 legal basis the vice chair had to direct the
2 state secretaries of state to send this
3 information to the proposed military website.
4 And this, by the way, is entirely apart from the
5 factual concerns that have been raised about the
6 adequacy of the security techniques that are
7 deployed with this site for personal
8 information.

9 THE COURT: All right. Let me get back,
10 then, in terms of looking at the -- back to the
11 standing issues in terms of -- you've
12 indicated -- if you want to respond to what she
13 indicated, why you would not be under the theory
14 that it requires that there be this assessment
15 before you collect -- no, it's the
16 organizational. Excuse me. The organizational
17 in terms of your public interest activities.

18 She indicated that -- and there was a
19 distinction in terms of what are considered in
20 that Public Interest Activities, what are
21 allowed and what are not allowed in terms of
22 providing you under this PETA case theory
23 organizational standing.

24 If you want to respond to -- that's where
25 your activities don't fit it.

1 MR. ROTENBERG: Right. Well, I think we've
2 done this, Your Honor, in our reply brief, if I
3 can just point to pages 20 and 21. In fact, we
4 are relying on PETA in making the argument that
5 we do have organizational standing and the
6 activities we describe is the participation and
7 work of our experts and to seek records from the
8 Commission and to respond to the requests that
9 had been made by the public.

10 What the language from PETA is relevant on
11 this point is that our activities are, quote,
12 "In response to and to counteract the effects of
13 defendant's alleged unlawful conduct."

14 That's page 20 in the reply.

15 THE COURT: All right. The other question
16 that I had is -- obviously, there needs to be
17 some sort of federal agency connection to the
18 Commission in order for the E-Gov Act to apply.
19 So what is your best argument as to what federal
20 agency is associated with it?

21 MR. ROTENBERG: Well, we think the
22 Commission itself is an agency for purposes of
23 the E-Government Act. That agency tracks the
24 definition of the Freedom of Information Act and
25 includes the Executive Office of the President.

1 So, therefore, the obligation to complete the
2 Privacy Impact Assessment would fall upon the
3 Commission as an agency.

4 THE COURT: You know, there is a case that
5 talks about -- and I forgot which of the -- it
6 was in the, I believe, the vice president's
7 office, and it indicated that they provided
8 basically personnel issues, those kinds of
9 assistance. It was the executive office of
10 either the president or the vice president. I
11 forgot which, and it was -- that commission had
12 not viewed itself as a federal agency.

13 MR. ROTENBERG: I'm not familiar with the
14 case, Your Honor. If we could find the cite, we
15 would be happy to provide a response.

16 I do want to point out, also --

17 THE COURT: Let me find it for you. It was
18 *Crew vs. The Office Of Administration*. It was
19 the Office of Administration within the
20 Executive Office of the President. In fact, it
21 was one of my cases relating to disclosure of
22 documents to the White House's alleged loss of
23 millions of emails, and they found that that
24 commission, based on its functions, was not --
25 you know, was not considered a federal agency

1 for different purposes.

2 MR. ROTENBERG: All right. But I don't
3 think that case implicated either the
4 E-Government Act or the Federal Advisory
5 Committee Act. So at least in the first
6 instance, we would need to look at whether those
7 statutes are relevant in Crew. I would be happy
8 to look more closely, Your Honor.

9 THE COURT: Okay. So besides indicating
10 that you think the Commission itself is a
11 federal agency, any other argument?

12 MR. ROTENBERG: Well, yes. The GSA, in
13 providing functional services to the Commission,
14 which, as we set out we believe is the
15 expectation contained within the executive order
16 and also the charter of the Commission, would be
17 subject to the agency status. And as you have
18 also suggested, the member of the EAC, by virtue
19 of the association with the EAC, could raise
20 agency concerns.

21 We found it interesting, for example, that
22 the Election Assistance Commission, not this
23 commission, but the one that Ms. McCormick is a
24 member of, has been subject to scrutiny under
25 the Privacy Impact Assessment by that agency's

1 Office of Inspector General for similar
2 activity.

3 Now, there's no wrongdoing. That's not
4 what I'm suggesting. But, rather, the point
5 being with far less data collection at the EAC,
6 for more than 10 years the Office of Inspector
7 General has paid careful attention to the
8 E-Government obligation. That is my point.

9 THE COURT: But the problem, at least as
10 she presents -- as Ms. Federighi presents it, is
11 that the person that's on the Commission is not
12 there in her official capacity.

13 MR. ROTENBERG: That's the representation.

14 THE COURT: Well, I know, but do you have
15 something to counter it?

16 MR. ROTENBERG: Well, the person who is on
17 the Commission is also affiliated with the most
18 significant election commission apart from the
19 president's commission that would address these
20 issues.

21 THE COURT: Do you think -- the Department
22 of Defense is not a defendant in this case, but
23 is there any argument as we pursued this issue
24 of the DOD having basically the website and all
25 of this material uploaded to it and maintaining

1 it at least for a period of time until it gets
2 transferred?

3 MR. ROTENBERG: Well --

4 THE COURT: Is that an agency that you
5 would argue is involved with the Commission or
6 not? Do you agree with the argument that it's
7 not?

8 MR. ROTENBERG: We would say that, in fact,
9 it is involved by virtue of the letter from the
10 vice chair. But by law, under the executive
11 order, it should not be involved. The fact that
12 it is receiving data, and is most certainly
13 subject to the Government Act as is evidenced by
14 the fact they've already had a Privacy Impact
15 Assessment, that is relevant. But the Privacy
16 Impact Assessment reveals that the military
17 website is not set up to receive the personal
18 data that the vice chairman is seeking.

19 THE COURT: Well, I'm trying to see
20 whether there is -- you agree with her argument
21 that you view that it shouldn't be there. That
22 doesn't get me anywhere in terms of your
23 argument that the Commission is subject to the
24 E-Gov Act. I still need a connection to a
25 federal agency. So I'm just trying to figure

1 out whether that's an argument you're making or
2 not making.

3 MR. ROTENBERG: Yes. Well, I would rely in
4 part on opposing counsel's comment that the
5 State of Arkansas has, in fact, transmitted
6 voter data to the military website. So the fact
7 that the military website is now in possession
8 of that data beyond what the authorities
9 provided in the Privacy Impact Assessment under
10 which it is currently operating, and we would
11 argue as well beyond the authority set out in
12 the executive order in the Commission charter,
13 necessarily makes it relevant to the proceeding.

14 THE COURT: All right. Anything else
15 either one of you wants to say? I'm going to
16 take a very short break. I know we're at 5:00,
17 but I need to take a short break and figure out
18 what additional questions, if any, I want to
19 make because I would like to have this be the
20 only hearing, and I'll go through all the
21 information that you've got and then make a
22 ruling.

23 MR. ROTENBERG: Thank you, Your Honor.

24 Just very briefly. We raised five counts.
25 There is the Privacy Impact Assessment that

1 should've been completed. There's the Privacy
2 Impact Assessment that was required as a
3 condition of receiving the data. There is the
4 obligation to publish that privacy impact under
5 the Federal Advisory Committee Act, and we
6 believe the informational privacy constitutional
7 claims are actually quite strong here, and we
8 would like the opportunity at some point to be
9 able --

10 THE COURT: At this point, to make a
11 constitutional argument I don't think you're
12 going to do well in this circuit.

13 MR. ROTENBERG: I understand, Your Honor.
14 Thank you.

15 THE COURT: Okay.

16 Anything you want to say at the end? I'm
17 going to hear whatever you have to say, and then
18 I need to take a quick break and look through
19 and make sure -- I did a scramble of a bunch of
20 notes because you've been filing things one
21 after the other in terms of my being able to
22 look through it to make sure that this is it and
23 I have the information I need.

24 MS. SHAPIRO: Yes. Just very briefly. I
25 just wanted to make two points. One is that

1 using the SAFE site as a tool I don't think
2 makes that part of the Commission's work. It
3 would be like saying that the Commission can use
4 the post office to mail letters because that
5 would make the post office somehow part of the
6 Commission. It is a tool for getting the
7 information.

8 THE COURT: Well, it's not getting the
9 information. I mean, as a practical matter --
10 are you talking about the computer? The DOD
11 thing?

12 MS. SHAPIRO: Yes.

13 THE COURT: Well, you're uploading it.
14 They're maintaining the information. I don't
15 know that I'd call it a tool as the post office
16 would be.

17 I would agree, mailing things through the
18 post office is not going to make them a federal
19 agency as part of the Commission.

20 MS. SHAPIRO: And my second point is I
21 wanted to just make clear the cases that set out
22 the tests for the agency requirements, in other
23 words, the functional test. The case that you
24 referred to, the *Crew vs. Office Of*
25 *Administration*, the case that Your Honor

1 handled, that involved the Office of
2 Administration within the Executive Office of
3 the President, was determined not to be an
4 agency subject to FOIA. And the E-Government
5 Act uses the same definition. That's the point
6 I wanted to make clear, that the definition of
7 agency is the same that's in FOIA. So the whole
8 including the Executive Office of the President,
9 we go back to the line of cases of *Soucie v.*
10 *David, Mayer v. Bush*, which I think is the task
11 force that Your Honor was referring to. That
12 was the deregulation Reagan task force with the
13 vice president as chair. So you have the *Mayer*
14 *v. Bush*, the *Soucie vs. David*.

15 So all of those cases mean that the
16 E-Government Act has to apply that same body of
17 case law, and there's -- the functional test
18 that's described in our papers, and we think is
19 very clear that it's not satisfied here.

20 And the Armstrong case, in addition, makes
21 it clear that just the mere participation of one
22 person doesn't change the character.

23 THE COURT: Okay. Let me take a short
24 break. I'll figure out if there's anything
25 else, and I'll come back out.

1 MS. SHAPIRO: Thank you.

2 (Break.)

3 THE COURT: I have just one last question.
4 I have not had an opportunity to review really
5 carefully the last missive that I received from
6 plaintiffs. I did look quickly through and
7 noticed the DOD impact statement. So I need to
8 go through and look at all of it more carefully.
9 But if on reflection, in looking at it and
10 reviewing the cases again and considering the
11 arguments that were made and the answers that
12 were given, if I decide that DOD is the federal
13 agency connection to the Commission, since DOD
14 is not a defendant, does it have to be a
15 defendant in order for the Court to basically --
16 assuming I find standing -- to be able to issue
17 any kind of order since they're the ones at this
18 point maintaining the data on behalf of the
19 Commission?

20 They're not a defendant now. Would they
21 have to be if I made that decision? I'm not
22 saying I'm going to. I'm just saying if I
23 decided to do it.

24 Anybody have a position on that?

25 MR. ROTENBERG: Of course, we just learned

1 this afternoon that the DOD now possesses data.
2 So we could quickly amend our complaint and add
3 the DOD as a named defendant.

4 THE COURT: Okay. Any position from DOJ on
5 this?

6 MS. SHAPIRO: Our position would be that
7 the Court would not be empowered to enter relief
8 against a nonparty so that --

9 THE COURT: Right. Okay. He would have to
10 make a decision as to whether he wanted to amend
11 the complaint. Let's assume he filed a motion
12 to amend the complaint which would include DOD,
13 what would your position be?

14 MS. SHAPIRO: That it --

15 THE COURT: I mean, presumably, at this
16 point they possess data, right? And they're
17 maintaining it, at least at this point?

18 MS. SHAPIRO: For some ephemeral amount of
19 time.

20 THE COURT: But they still have it at this
21 point. So if they decided to amend it, I mean,
22 then the Court would have to see whether that
23 works anyway. But I'm just saying that it's
24 clear that if they're not a party, I would not
25 be able to act if I thought that was the -- or

1 concluded that that was the federal agency
2 connection.

3 So if they filed a motion to do it, what
4 would your answer be?

5 MS. SHAPIRO: Well, I think we would
6 respond with arguments similar that the DOD tool
7 that is being used does not convert -- make any
8 difference to the agency -- to the Commission's
9 status as a non-agency or a requirement to do a
10 Privacy Impact Assessment.

11 THE COURT: So that would -- all right. In
12 terms of doing it, but it doesn't get to
13 whether -- even if he decided to put it in, it
14 doesn't mean that he necessarily will decide
15 that.

16 So it seems to me, since at this point they
17 do have the data, and they're maintaining it,
18 that they could certainly have grounds to put
19 them in as a party. It doesn't mean I
20 necessarily am going to find, as they would
21 hope, that that is the federal agency
22 connection. But I just wanted to make sure if I
23 started to go down that path, it actually
24 could -- it could be any ruling.

25 MS. SHAPIRO: I'm sorry. I didn't

1 understand the last --

2 THE COURT: All right. I brought this up
3 because this has been a more developed argument
4 about DOD and its role, since that's come out
5 really only in recent times, and the exhibit I
6 got at 3:00. So I haven't had too long to look
7 at it in terms of what's involved with it. And
8 you have indicated that it, at this point, holds
9 data from the State of Arkansas. So it has the
10 information, and it's maintaining it on behalf
11 of the Commission. So that presumably would be
12 their reason to amend it. The Court would still
13 have to make these other decisions. It doesn't
14 change it.

15 MS. SHAPIRO: Correct.

16 THE COURT: I just want to see that if I
17 decided to do that, that I actually would be in
18 a position to do it.

19 MS. SHAPIRO: Okay.

20 THE COURT: All right. So if you're going
21 to amend it, you need to move swiftly. All
22 right. I don't have anything else, and so I
23 will excuse you.

24 I will not be doing an oral ruling.
25 Obviously, it's very complicated. I will be

1 doing something in writing. I will get it out
2 as quickly as I can understanding the time lines
3 that have been set out.

4 All right? Thank you. Take care.

5 (Hearing concluded.)
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 CERTIFICATE OF REPORTER

2
3 I, Richard D. Ehrlich, a Registered Merit
4 Reporter and Certified Realtime Reporter,
5 certify that the foregoing is a true, complete,
6 and accurate transcript of the proceedings
7 ordered to be transcribed in the above-entitled
8 case before the Honorable Colleen
9 Kollar-Kotelly, in Washington, DC, on July 7,
10 2017.

11
12 s/Richard D. Ehrlich July 10, 2017

13

Richard D. Ehrlich, Official Court Reporter
14
15
16
17
18
19
20
21
22
23
24
25

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.

Civil Action No. 1:17-cv-1320 (CKK)

THIRD DECLARATION OF KRIS W. KOBACH

I, Kris W. Kobach, declare as follows:

As described in my declaration of July 5, 2017, I am the Vice Chair of the Presidential Advisory Commission on Election Integrity (“Commission”). I submit this third declaration in support of Defendant’s supplemental brief regarding the addition of the Department of Defense (“DOD”) as a defendant in plaintiff’s Amended Complaint. This declaration is based on my personal knowledge and upon information provided to me in my official capacity as Vice Chair of the Commission.

1. In order not to impact the ability of other customers to use the DOD Safe Access File Exchange (“SAFE”) site, the Commission has decided to use alternative means for transmitting the requested data. The Commission no longer intends to use the DOD SAFE system to receive information from the states, and instead intends to use alternative means of receiving the information requested in the June 28, 2017, letter. Specifically, the Director of White House Information Technology is repurposing an existing system that regularly accepts

personally identifiable information through a secure, encrypted computer application within the White House Information Technology enterprise. We anticipate this system will be fully functional by 6:00 p.m. Eastern today.

2. Today, the Commission sent the states a follow-up communication requesting the states not submit any data until this Court rules on this TRO motion. A copy of this communication is attached hereto as Exhibit A. The Commission will not send further instructions about how to use the new system pending this Court's resolution of this TRO motion.

3. The Commission will not download the data that Arkansas already transmitted to SAFE and this data will be deleted from the site.

4. Additionally, I anticipate that the President will today announce the appointment of two new members of the Commission, one Democrat and one Republican.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 10th day of July 2017.



Kris W. Kobach

From: FN-OVP-Election Integrity Staff

Sent: Monday, July 10, 2017 9:40 AM

Subject: Request to Hold on Submitting Any Data Until Judge Rules on TRO

Dear Election Official,

As you may know, the Electronic Privacy Information Center filed a complaint seeking a Temporary Restraining Order (“TRO”) in connection with the June 28, 2017 letter sent by Vice Chair Kris Kobach requesting publicly-available voter data. See *Electronic Privacy Information Center v. Presidential Advisory Commission on Election Integrity* filed in the U.S. District Court for the District of Columbia. Until the Judge rules on the TRO, we request that you hold on submitting any data. We will follow up with you with further instructions once the Judge issues her ruling.

Andrew Kossack

Designated Federal Officer

Presidential Advisory Commission on Election Integrity

ElectionIntegrityStaff@ovp.eop.gov

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

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009

Plaintiff,

v.

Civ. Action No. 17-1320 (CKK)

PRESIDENTIAL ADVISORY COMMISSION ON
ELECTION INTEGRITY; MICHAEL PENCE, in his
official capacity as Chair of the Presidential Advisory
Commission on Election Integrity; KRIS KOBACH, in his
official capacity as Vice Chair of the Presidential Advisory
Commission on Election Integrity; CHARLES C.
HERNDON, in his official capacity as Director of White
House Information Technology; EXECUTIVE OFFICE
OF THE PRESIDENT OF THE UNITED STATES;
OFFICE OF THE VICE PRESIDENT OF THE UNITED
STATES; UNITED STATES DIGITAL SERVICE;
EXECUTIVE COMMITTEE FOR PRESIDENTIAL
INFORMATION TECHNOLOGY;
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

GENERAL SERVICES ADMINISTRATION
1800 F Street, N.W.
Washington, D.C. 20405

UNITED STATES DEPARTMENT OF DEFENSE
1000 Defense Pentagon
Washington, D.C. 20301-0001

Defendants.

SECOND AMENDED COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Administrative Procedure Act (“APA”), 5 U.S.C. §§ 551–706, the Federal Advisory Committee Act (“FACA”), 5 U.S.C. app. 2, and the United States Constitution for injunctive and other appropriate relief to halt the collection of state voter data by the Presidential Advisory Commission on Election Integrity (the “PACEI” or the “Commission”), by officers of the Commission, and by the agencies which oversee and facilitate the activities of the Commission, including the Department of Defense.

2. The Electronic Privacy Information Center (“EPIC”) challenges the Defendants’ intent to collect the personal data of millions of registered voters and to publish partial SSNs as an unconstitutional invasion of privacy and a violation of the obligation to conduct a Privacy Impact Assessment (“PIA”).

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, 5 U.S.C. § 702, and 5 U.S.C. § 704. This Court has personal jurisdiction over Defendants.

4. Venue is proper in this district under 5 U.S.C. § 703 and 28 U.S.C. § 1391.

Parties

5. Plaintiff EPIC is a nonprofit organization incorporated in Washington, D.C., and established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC’s mission is oversight and analysis of government activities. EPIC’s Advisory Board members include distinguished experts in law, technology, public policy, and cybersecurity. EPIC has a long history of working to protect voter privacy and the security of election infrastructure. EPIC has specific expertise regarding the misuse of the Social Security Number (“SSN”) and has sought stronger protections for the SSN for more than two decades.

6. EPIC’s members include registered voters in California, the District of Columbia, Florida, Maryland, Massachusetts, Minnesota, New York, Pennsylvania, Texas, and Washington.

7. Defendant PACEI is an advisory committee of the U.S. government within the meaning of FACA, 5 U.S.C. app. 2 § 10. Defendant PACEI is also an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

8. Defendant Michael Pence is the Vice President of the United States and the Chair of the PACEI.

9. Defendant Kris Kobach is the Secretary of State of Kansas and the Vice Chair of the PACEI.

10. Defendant Charles C. Herndon is the Director of White House Information Technology.

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

12. Defendant U.S. Digital Service is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

13. Defendant Executive Committee for Presidential Information Technology consists of the following officials or their designees: 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 Services; and the Director of the White House Military Office. The Executive Committee is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

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

15. Defendant General Services Administration (“GSA”) is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The GSA is charged with providing the PACEI

“such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission” Ex. 1.¹

16. Defendant United States Department of Defense (“DoD”) is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The DoD manages and controls the Safe Access File System (“SAFE”).

Facts

The Commission’s Unprecedented Collection of State Voter Data

17. The Commission was established by Executive Order on May 11, 2017 (“Commission Order”). Ex 1.²

18. The Commission is charged with “study[ing] the registration and voting processes used in Federal elections.” Ex. 1.³ The Commission Order contains no authority to gather personal data or to undertake investigations.⁴

19. On June 28, 2017, the Vice Chair of the Commission undertook to collect detailed voter histories from all fifty states and the District of Columbia. Such a request had never been made by any federal official in the history of the country. The Vice Chair stated during a phone call with Commission members that “a letter w[ould] be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls” Ex. 2.⁵

¹ Exec. Order. No. 13,799, 82 Fed. Reg. 22,389, 22,390 (May 11, 2017).

² 82 Fed. Reg. at 22,389; *see also Voter Privacy and the PACEI*, EPIC.org (June 30, 2017), <https://epic.org/privacy/voting/pacei/>.

³ 82 Fed. Reg. at 22,389.

⁴ *See generally id.*

⁵ Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017).

20. According to the U.S. Census, state voter rolls include the names, addresses, and other personally identifiable information of at least 157 million registered voters.⁶

21. One of the letters from the Commission, dated June 28, 2017, was sent to North Carolina Secretary of State Elaine Marshall. Ex. 3.⁷

22. In the letter (“Commission Letter”), the Vice Chair urged the Secretary of State 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.” Ex. 3.⁸

23. The Commission Letter also asked “[w]hat evidence or information [the state had] regarding instances of voter fraud or registration fraud” and “[w]hat convictions for election-related crimes ha[d] occurred in [the] state since the November 2000 federal election.” Ex. 3.⁹

24. The Commission Letter stated that “any documents that are submitted to the full Commission w[ould] also be made available to the public.” Ex. 3.¹⁰

25. The Commission asked for a response by July 14, 2017. Ex. 3.¹¹ The “SAFE” URL, recommend by the Commission for the submission of voter data, leads election officials to a non-

⁶ U.S. Census Bureau, *Voting and Registration in the Election of November 2016* at tbl. 4a (May 2017), <https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html>.

⁷ Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017).

⁸ *Id.* at 1–2.

⁹ *Id.* at 1.

¹⁰ *Id.* at 2.

¹¹ *Id.*

secure site. Regarding this website, Google Chrome states: “Your connection is not private. Attackers may be trying to steal your information from [the site proposed by the Commission] (for example, passwords, messages, or credit cards).” Ex. 4.¹²

26. As of July 7, 2017, the Department of Defense has received voter data from at least one state, Arkansas, in the SAFE system.

27. According to representations made by the Commission in the July 10, 2017 response, the Commission sent a “Follow-up Communication” to the states, requesting that the States not submit any data until this Court rules on EPIC’s motion for a temporary restraining order.

28. The Follow-up Communication from the Commission to the States was not made public as would be required by the Federal Advisory Committee Act.

29. There is no public confirmation that all of the States received the Follow-up Communication from the Commission.

30. There is no public confirmation that the States that did receive the Follow-up Communication will comply.

31. According to representations made by the Commission in the July 10, 2017 response, the Director of White House Information Technology is “repurposing” a computer system to be used for collecting personal voter data.

32. On July 10, 2017, the Commission stated that it would not send further instructions about how to use the new system pending the Court’s resolution of EPIC’s motion for a temporary restraining order.

¹² Screenshot: Google Chrome Security Warning for Safe Access File Exchange (“SAFE”) Site (July 3, 2017 12:02 AM).

33. On July 10, 2017, the Commission stated that it would not download the data that Arkansas already transmitted via the DoD system, and that the data will be deleted from the site. There has been no confirmation that the data has been deleted.

The General Service Administration’s Role in Providing Support to the Commission

34. 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.”¹³

35. 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.”¹⁴

36. The GSA routinely conducts and publishes Privacy Impact Assessments when it collects, maintains, and uses personal information on individuals.¹⁵

37. 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.”

Many States Oppose the Commission’s Demand for Personal Voter Data

38. In less than three days following the release of the Commission Letter, election officials in twenty-four states said that they would oppose, partially or fully, the demand for personal voter data.¹⁶

¹³ 82 Fed. Reg. at 22,390.

¹⁴ Charter, Presidential Advisory Commission on Election Integrity ¶ 6.

¹⁵ *Privacy Impact Assessments*, GSA (Apr. 13, 2017), <https://www.gsa.gov/portal/content/102237>.

39. California Secretary of State Alex Padilla stated that he would “not provide sensitive voter information to a committee that has already inaccurately passed judgment that millions of Californians voted illegally. California’s participation would only serve to legitimize the false and already debunked claims of massive voter fraud.”¹⁷

40. Kentucky Secretary of State Alison Lundergan Grimes stated that “Kentucky w[ould] not aid a commission that is at best a waste of taxpayer money and at worst an attempt to legitimize voter suppression efforts across the country.”¹⁸

41. Virginia Governor Terry McAuliffe stated that he had “no intention of honoring [Kobach’s] request.”¹⁹

42. More than fifty experts in voting technology and twenty privacy organizations wrote to state election officials to warn that “[t]here is no indication how the information will be used, who will have access to it, or what safeguards will be established.”²⁰

Failure to Conduct a Privacy Impact Assessment

¹⁶ Philip Bump & Christopher Ingraham, *Trump Says States Are ‘Trying to Hide’ Things from His Voter Fraud Commission. Here’s What They Actually Say*, Wash. Post (July 1, 2017), <https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/>.

¹⁷ Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017), <http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/>.

¹⁸ Bradford Queen, Secretary Grimes Statement on Presidential Election Commission's Request for Voters' Personal Information, Kentucky (last accessed July 3, 2017) <http://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prId=129>.

¹⁹ Terry McAuliffe, *Governor McAuliffe Statement on Request from Trump Elections Commission* (June 29, 2017), <https://governor.virginia.gov/newsroom/newsarticle?articleId=20595>.

²⁰ Letter from EPIC et al. to Nat’l Ass’n of State Sec’y’s (July 3, 2017), <https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf>.

43. Under the E-Government Act of 2002,²¹ 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.²²

44. The agency must “(i) conduct 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.”²³

45. The Commission is an agency subject to the E-Government Act because it is an “establishment in the executive branch of the Government,” a category which “includ[es] the Executive Office of the President.”²⁴

46. The Executive Office of the President is an agency subject to the E-Government Act.

47. The U.S. Digital Service is an agency subject to the E-Government Act.

48. The Director of White House Information Technology is subject to the E-Government Act.

49. The Director of White House Information Technology was established in 2015 and has “the primary authority to establish and coordinate the necessary policies and procedures for

²¹ Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note).

²² 44 U.S.C. § 3501 note (“Privacy Impact Assessments”).

²³ *Id.*

²⁴ 44 U.S.C. § 3502(1).

operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP.”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.”²⁶

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 under this memorandum.”²⁷

50. The Director has the independent authority to oversee and “provide the necessary advice, coordination, and guidance to” the Executive Committee for Presidential Information Technology, which “consists of the following officials or their designees: 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.”²⁸

51. A Privacy Impact Assessment for a “new collection of information” must be “commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information.”²⁹ The PIA must specifically address “(I) what information is to be

²⁵ 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), attached as Ex. 5.

²⁶ *Id.* § 2(c).

²⁷ *Id.* § 2(d).

²⁸ *Id.* § 3.

²⁹ 44 U.S.C. § 3501 note (“Privacy Impact Assessments”).

collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and] (VI) how the information will be secured”³⁰

52. Under the FACA, “records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [an] advisory committee shall be available for public inspection and copying at a single location in the offices of the advisory committee or the agency to which the advisory committee reports until the advisory committee ceases to exist.”³¹

53. None of the Defendants have conducted a Privacy Impact Assessment for the Commission’s collection of state voter data.

54. None of the Defendants have ensured review of a PIA by any Chief Information Officer or equivalent official.

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

The DoD’s Privacy Impact Assessment Does Not Permit
the Collection of Personal Information from The General Public

56. The DoD last approved a PIA for the Safe Access File Exchange system in 2015.³²

57. The 2015 PIA indicates that the SAFE system may “collect, maintain, use and/or disseminate PII” about only “federal personnel and/or federal contractors.”³³

³⁰ *Id.*

³¹ 5 U.S.C. app. 2 § 10(b).

³² Army Chief Information Officer, U.S. Dep’t of Def., *Privacy Impact Assessments* (April 27, 2016), <http://ciog6.army.mil/PrivacyImpactAssessments/tabid/71/Default.aspx>.

³³ EPIC Supp. Ex. 5, ECF No. 20-1, at 1.

58. The 2015 PIA specifically indicates that the SAFE system may not be used to “collect, maintain, use and/or disseminate PII” from “members of the general public.”³⁴

59. According to the 2015 PIA, the SAFE system may not be used to collect the data set out in the June 28, 2017, from Vice Chair Kobach, directing state election officials to provide voter roll data.

60. The DoD has not issued a PIA for the collection of personal data from the general public.

61. The DoD has not issued a PIA that would permit the receipt of data specified in the June 28, 2017, Kobach letter.

Count I

Violation of APA: Unlawful Agency Action

62. Plaintiff asserts and incorporates by reference paragraphs 1–42.

63. Defendants’ collection of state voter data prior to creating, reviewing, and publishing a Privacy Impact Assessment, 44 U.S.C. § 3501 note, is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law under 5 U.S.C. § 706(2)(a) and short of statutory right under 5 U.S.C. § 706(2)(c).

64. Defendants’ decision to initiate collection of voter data is a final agency action within the meaning of 5 U.S.C. § 704.

65. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants’ actions.

66. Plaintiff has exhausted all applicable administrative remedies.

Count II

Violation of APA: Agency Action Unlawfully Withheld

³⁴ EPIC Supp. Ex. 5, ECF No. 20-1, at 1.

67. Plaintiff asserts and incorporates by reference paragraphs 1–42.
68. Defendants have failed to create, review, and/or publish a privacy impact assessment for Defendants’ collection of voter data, as required by 44 U.S.C. § 3501 note and 5 U.S.C. app. 2 § 10(b).
69. Defendants’ failure to take these steps constitutes agency action unlawfully withheld or unreasonably delayed in violation of 5 U.S.C. § 706(1).
70. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants’ actions and inaction.
71. Plaintiff has exhausted all applicable administrative remedies.

Count III

Violation of FACA: Failure to Make Documents Available for Public Inspection

72. Plaintiff asserts and incorporates by reference paragraphs 1–42.
73. Defendants have failed to make available for public inspection a privacy impact assessment for the collection of voter data.
74. Defendants’ failure to make available for public inspection a PIA required by law is a violation of 5 U.S.C. app. 2 § 10(b).
75. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants’ actions and inaction.
76. Plaintiff has exhausted all applicable administrative remedies.

Count IV

Violation of Fifth Amendment: Substantive Due Process/Right to Informational Privacy

77. Plaintiff asserts and incorporates by reference paragraphs 1–42.

78. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have violated the informational privacy rights of millions of Americans, including members of the EPIC Advisory Board, guaranteed by the Due Process Clause of the Fifth Amendment. *See* U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

79. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

Count V

Violation of Fifth Amendment: Procedural Due Process

80. Plaintiff asserts and incorporates by reference paragraphs 1–42.

81. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have deprived EPIC's members of their liberty interest in avoiding the disclosure of personal matters. U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

82. Defendants have done so without providing notice to EPIC's members, without providing EPIC's members an opportunity to challenge the collection of their personal data, and without providing for a neutral decisionmaker to decide on any such challenges brought by EPIC's members.

83. Defendants have violated EPIC's members Fifth Amendment right to due process of law. U.S. Const. amend. V.

84. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

Requested Relief

WHEREFORE, Plaintiff requests that this Court:

- A. Hold unlawful and set aside Defendants' authority to collect personal voter data from the states;
- B. Order Defendants to halt collection of personal voter data;
- C. Order Defendants to securely delete and properly disgorge any personal voter data collected or subsequently received;
- D. Order Defendants to promptly conduct a privacy impact assessment prior to the collection of personal voter data;
- E. Award EPIC costs and reasonable attorney's fees incurred in this action; and
- F. Grant such other relief as the Court may deem just and proper.

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 11, 2017

This is historical material, "frozen in time" and not current OMB guidance.
The web site is no longer updated and links to external web sites and some internal pages will not work.



September 26, 2003

M-03-22

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

A handwritten signature in blue ink, appearing to read "JB", is placed to the right of the name and title.

SUBJECT: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

The attached guidance provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

The Administration is committed to protecting the privacy of the American people. This guidance document addresses privacy protections when Americans interact with their government. The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, cyberspace security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in the federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

Background

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act (see Attachment A). The text of section 208 is provided as Attachment B to this Memorandum. Attachment C provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA"). Attachment D summarizes the modifications to existing guidance resulting from this Memorandum. A complete list of OMB privacy guidance currently in effect is available at OMB's website.

As OMB has previously communicated to agencies, for purposes of their FY2005 IT budget requests, agencies should submit all required Privacy Impact Assessments no later than October 3, 2003.

For any questions about this guidance, contact Eva Kleederman, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, fax (202) 395-5167, e-mail Eva_Kleederman@omb.eop.gov.

Attachments

[Attachment A](#)
[Attachment B](#)
[Attachment C](#)
[Attachment D](#)

Attachment A

E-Government Act Section 208 Implementation Guidance

I. General

A. **Requirements.** Agencies are required to:

1. conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available (see Section II of this Guidance),
2. post privacy policies on agency websites used by the public (see Section III),
3. translate privacy policies into a standardized machine-readable format (see Section IV), and
4. report annually to OMB on compliance with section 208 of the E-Government Act of 2002 (see Section VII).

B. **Application.** This guidance applies to:

1. all executive branch departments and agencies (“agencies”) and their contractors that use information technology or that operate websites for purposes of interacting with the public;
2. relevant cross-agency initiatives, including those that further electronic government.

C.

Modifications to Current Guidance. Where indicated, this Memorandum modifies the following three memoranda, which are replaced by this guidance (see summary of modifications at Attachment D):

1. [Memorandum 99-05](#) (January 7, 1999), directing agencies to examine their procedures for ensuring the privacy of personal information in federal records and to designate a senior official to assume primary responsibility for privacy policy;
2. [Memorandum 99-18](#) (June 2, 1999), concerning posting privacy policies on major entry points to government web sites as well as on any web page collecting substantial personal information from the public; and
3. [Memorandum 00-13](#) (June 22, 2000), concerning (i) the use of tracking technologies such as persistent cookies and (ii) parental consent consistent with the Children’s Online Privacy Protection Act (“COPPA”).

II. Privacy Impact Assessment

A. **Definitions.**

1. *Individual* - means a citizen of the United States or an alien lawfully admitted for permanent residence.¹
2. *Information in identifiable form*- is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).²
3. *Information technology (IT)* - means, as defined in the Clinger-Cohen Act³, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
4. *Major information system* - embraces “large” and “sensitive” information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency’s programs, finances, property or other resources.
5. *National Security Systems* - means, as defined in the Clinger-Cohen Act⁴, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.
6. *Privacy Impact Assessment (PIA)*- 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.
7. *Privacy policy in standardized machine-readable format*- means a statement about site privacy

practices written in a standard computer language (not English text) that can be read automatically by a web browser.

B. When to conduct a PIA.⁵

1. *The E-Government Act requires agencies to conduct a PIA before:*
 - a. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
 - b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).
2. *In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:*
 - a. Conversions - when converting paper-based records to electronic systems;
 - b. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
 - c. Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
 - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
 - d. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
 - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
 - e. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
 - f. Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
 - g. New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
 - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.
 - h. Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
 - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
 - i. Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)
3. *No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged, as in the following circumstances:*
 - a. for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public (this includes government personnel and government contractors and consultants),⁶
 - b. for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or

- obtaining additional information;
 - c. for national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act);
 - d. when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act (see 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide privacy protection for matched information;
 - e. when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act of 2002;
 - f. if agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form;
 - g. for minor changes to a system or collection that do not create new privacy risks.
4. **Update of PIAs:** Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

C. Conducting a PIA.

1. Content.

- a. PIAs must analyze and describe:
 - i. what information is to be collected (e.g., nature and source);
 - ii. why the information is being collected (e.g., to determine eligibility);
 - iii. intended use of the information (e.g., to verify existing data);
 - iv. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
 - v. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
 - vi. how the information will be secured (e.g., administrative and technological controls⁷); and
 - vii. whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.
 - b. **Analysis:** PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
2. Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection:
- a. **Specificity.** The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.
 - i. **IT development stage.** PIAs conducted at this stage:
 - 1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
 - 2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;
 - 3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.
 - ii. **Major information systems.** PIAs conducted for these systems should reflect more extensive analyses of:
 - 1. the consequences of collection and flow of information,
 - 2. the alternatives to collection and handling as designed,
 - 3. the appropriate measures to mitigate risks identified for each alternative and,
 - 4. the rationale for the final design choice or business process.
 - iii. **Routine database systems.** Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.
 - b. **Information life cycle analysis/collaboration.** Agencies must consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. To be

comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.

3. *Review and publication.*

a. Agencies must ensure that:

- i. the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);
- ii. for each covered IT system for which 2005 funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300⁸); and
- iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).
 1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment⁹. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).
 2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

D. *Relationship to requirements under the Paperwork Reduction Act (PRA)*¹⁰.

1. Joint Information Collection Request (ICR) and PIA. Agencies undertaking new electronic information collections may conduct and submit the PIA to OMB, and make it publicly available, as part of the SF83 Supporting Statement (the request to OMB to approve a new agency information collection).
2. If Agencies submit a Joint ICR and PIA:
 - a. All elements of the PIA must be addressed and identifiable within the structure of the Supporting Statement to the ICR, including:
 - i. a description of the information to be collected in the response to Item 1 of the Supporting Statement¹¹;
 - ii. a description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement¹²;
 - iii. a statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement¹³;
 - iv. a discussion in item 10 of the Supporting Statement of:
 1. whether individuals are informed that providing the information is mandatory or voluntary
 2. opportunities to consent, if any, to sharing and submission of information;
 3. how the information will be secured; and
 4. whether a system of records is being created under the Privacy Act¹⁴.
 - b. For additional information on the requirements of an ICR, please consult your agency's organization responsible for PRA compliance.
3. Agencies need not conduct a new PIA for simple renewal requests for information collections under the PRA. As determined by reference to section II.B.2. above, agencies must separately consider the need for a PIA when amending an ICR to collect information that is significantly different in character from the original collection.

E. *Relationship to requirements under the Privacy Act of 1974, 5 U.S. C. 552a.*

1. Agencies may choose to conduct a PIA when developing the System of Records (SOR) notice required by subsection (e)(4) of the Privacy Act, in that the PIA and SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).
2. Agencies, in addition, may make the PIA publicly available in the Federal Register along with the Privacy Act SOR notice.

3. Agencies must separately consider the need for a PIA when issuing a change to a SOR notice (e.g., a change in the type or category of record added to the system may warrant a PIA).

III. Privacy Policies on Agency Websites

- A. *Privacy Policy Clarification.* To promote clarity to the public, agencies are required to refer to their general web site notices explaining agency information handling practices as the "Privacy Policy."
- B. *Effective Date.* Agencies are expected to implement the following changes to their websites by December 15, 2003.
- C. *Exclusions:* For purposes of web privacy policies, this guidance does not apply to:
 1. information other than "government information" as defined in [OMB Circular A-130](#);
 2. agency intranet web sites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees);
 3. national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-government Act).
- D. *Content of Privacy Policies.*
 1. Agency Privacy Policies must comply with guidance issued in OMB [Memorandum 99-18](#) and must now also include the following two new content areas:
 - a. *Consent to collection and sharing*¹⁵. Agencies must now ensure that privacy policies:
 - i. inform visitors whenever providing requested information is voluntary;
 - ii. inform visitors how to grant consent for use of voluntarily-provided information; and
 - iii. inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
 - b. *Rights under the Privacy Act or other privacy laws*¹⁶. Agencies must now also notify web-site visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (such as the Health Insurance Portability and Accountability Act of 1996, the IRS Restructuring and Reform Act of 1998, or the Family Education Rights and Privacy Act):
 - i. in the body of the web privacy policy;
 - ii. via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or
 - iii. via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).
 2. Agency Privacy Policies must continue to address the following, modified, requirements:
 - a. Nature, purpose, use and sharing of information collected . Agencies should follow existing policies (issued in [OMB Memorandum 99-18](#)) concerning notice of the nature, purpose, use and sharing of information collected via the Internet, as modified below:
 - i. *Privacy Act information.* When agencies collect information subject to the Privacy Act, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either:
 1. at the point of collection, or
 2. via link to the agency's general Privacy Policy¹⁸.
 - ii. *"Privacy Act Statements."* Privacy Act Statements must notify users of the authority for and purpose and use of the collection of information subject to the Privacy Act, whether providing the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.
 - iii. *Automatically Collected Information (site management data).* Agency Privacy Policies must specify what information the agency collects automatically (i.e., user's IP address, location, and time of visit) and identify the use for which it is collected (i.e., site management or security purposes).
 - iv. *Interaction with children:* Agencies that provide content to children under 13 and that collect personally identifiable information from these visitors should incorporate the requirements of the Children's Online Privacy Protection Act ("COPPA") into their Privacy Policies (see Attachment C)¹⁹.
 - v. *Tracking and customization activities.* Agencies are directed to adhere to the following modifications to [OMB Memorandum 00-13](#) and the OMB follow-up guidance letter dated [September 5, 2000](#):
 1. *Tracking technology prohibitions:*

- a. agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below;
 - b. agency heads may approve, or may authorize the heads of sub-agencies or senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's must post clear notice in the agency's privacy policy of:
 - the nature of the information collected;
 - the purpose and use for the information;
 - whether and to whom the information will be disclosed; and
 - the privacy safeguards applied to the information collected.
 - c. agencies must report the use of persistent tracking technologies as authorized for use by subsection b. above (see section VII)²⁰.
2. *The following technologies are not prohibited:*
- a. Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
 - b. Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see v.1.b above) and where the following is posted in the Agency's Privacy Policy:
 - the purpose of the tracking (i.e., customization of the site);
 - that accepting the customizing feature is voluntary;
 - that declining the feature still permits the individual to use the site; and
 - the privacy safeguards in place for handling the information collected.
 - c. Agency use of password access to information that does not involve "persistent cookies" or similar technology.
- vi. *Law enforcement and homeland security sharing:* Consistent with current practice, Internet privacy policies may reflect that collected information may be shared and protected as necessary for authorized law enforcement, homeland security and national security activities.
- b. *Security of the information*²¹. Agencies should continue to comply with existing requirements for computer security in administering their websites²² and post the following information in their Privacy Policy:
- i. in clear language, information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and
 - ii. in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)
- E. *Placement of notices.* Agencies should continue to follow the policy identified in [OMB Memorandum 99-18](#) regarding the posting of privacy policies on their websites. Specifically, agencies must post (or link to) privacy policies at:
1. their principal web site;
 2. any known, major entry points to their sites;
 3. any web page that collects substantial information in identifiable form.
- F. *Clarity of notices.* Consistent with [OMB Memorandum 99-18](#), privacy policies must be:
1. clearly labeled and easily accessed;
 2. written in plain language; and
 3. made clear and easy to understand, whether by integrating all information and statements into a single posting, by layering a short "highlights" notice linked to full explanation, or by other means the agency determines is effective.

IV. Privacy Policies in Machine-Readable Formats

A. *Actions.*

1. Agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make

an informed choice about whether to conduct business with that site.

2. OMB encourages agencies to adopt other privacy protective tools that become available as the technology advances.

B. **Reporting Requirement.** Agencies must develop a timetable for translating their privacy policies into a standardized machine-readable format. The timetable must include achievable milestones that show the agency's progress toward implementation over the next year. Agencies must include this timetable in their reports to OMB (see Section VII).

V. Privacy Policies Incorporated by this Guidance

In addition to the particular actions discussed above, this guidance reiterates general directives from previous OMB Memoranda regarding the privacy of personal information in federal records and collected on federal web sites. Specifically, existing policies continue to require that agencies:

- A. assure that their uses of new information technologies sustain, and do not erode, the protections provided in all statutes relating to agency use, collection, and disclosure of personal information;
- B. assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- C. evaluate legislative proposals involving collection, use and disclosure of personal information by the federal government for consistency with the Privacy Act of 1974;
- D. evaluate legislative proposals involving the collection, use and disclosure of personal information by any entity, public or private, for consistency with the Privacy Principles;
- E. ensure full adherence with stated privacy policies.

VI. Agency Privacy Activities/Designation of Responsible Official

Because of the capability of information technology to capture and disseminate information in an instant, all federal employees and contractors must remain mindful of privacy and their obligation to protect information in identifiable form. In addition, implementing the privacy provisions of the E-Government Act requires the cooperation and coordination of privacy, security, FOIA/Privacy Act and project officers located in disparate organizations within agencies. Clear leadership and authority are essential.

Accordingly, this guidance builds on policy introduced in Memorandum 99-05 in the following ways:

- A. Agencies must:
 1. inform and educate employees and contractors of their responsibility for protecting information in identifiable form;
 2. identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies.
 3. designate an appropriate senior official or officials (e.g., CIO, Assistant Secretary) to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies. The designated official(s) shall coordinate implementation of OMB web and privacy policy and guidance.
 4. designate an appropriate official (or officials, as appropriate) to serve as the "reviewing official(s)" for agency PIAs.
- B. OMB leads a committee of key officials involved in privacy that reviewed and helped shape this guidance and that will review and help shape any follow-on privacy and web-privacy-related guidance. In addition, as part of overseeing agencies' implementation of section 208, OMB will rely on the CIO Council to collect information on agencies' initial experience in preparing PIAs, to share experiences, ideas, and promising practices as well as identify any needed revisions to OMB's guidance on PIAs.

VII. Reporting Requirements

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report. The first reports are due to OMB by December 15, 2003. All agencies that use information technology systems and conduct electronic information collection activities must complete a report on compliance with this guidance, whether or not they submit budgets to OMB.

Reports must address the following four elements:

- A. *Information technology systems or information collections for which PIAs were conducted.* Include the mechanism by which the PIA was made publicly available (website, Federal Register, other), whether the PIA was made publicly available in full, summary form or not at all (if in summary form or not at all, explain), and, if made available in conjunction with an ICR or SOR, the publication date.
- B. *Persistent tracking technology uses.* If persistent tracking technology is authorized, include the need that

compels use of the technology, the safeguards instituted to protect the information collected, the agency official approving use of the tracking technology, and the actual privacy policy notification of such use.

- C. *Agency achievement of goals for machine readability*. Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.
- D. *Contact information*. Include the individual(s) (name and title) appointed by the head of the Executive Department or agency to serve as the agency's principal contact(s) for information technology/web matters and the individual (name and title) primarily responsible for privacy policies.

Attachment B
E-Government Act of 2002
Pub. L. No. 107-347, Dec. 17, 2002

SEC. 208. PRIVACY PROVISIONS.

A. **PURPOSE.** — The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

B. **PRIVACY IMPACT ASSESSMENTS.**—

1. **RESPONSIBILITIES OF AGENCIES.**—

- a. **IN GENERAL.**—An agency shall take actions described under subparagraph (b) before—
 - i. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
 - ii. initiating a new collection of information that—
 - 1. will be collected, maintained, or disseminated using information technology; and
 - 2. 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.
- b. **AGENCY ACTIVITIES.** —To the extent required under subparagraph (a), each agency shall—
 - i. conduct 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.
- c. **SENSITIVE INFORMATION.** —Subparagraph (b)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.
- d. **COPY TO DIRECTOR.** —Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

2. **CONTENTS OF A PRIVACY IMPACT ASSESSMENT.** —

- a. **IN GENERAL.** —The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.
- b. **GUIDANCE.** — The guidance shall—
 - i. 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
 - ii. require that a privacy impact assessment address—
 - 1. what information is to be collected;
 - 2. why the information is being collected;
 - 3. the intended use of the agency of the information;
 - 4. with whom the information will be shared;
 - 5. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
 - 6. how the information will be secured; and
 - 7. whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the 'Privacy Act').

3. **RESPONSIBILITIES OF THE DIRECTOR.**—The Director shall—

- a. develop policies and guidelines for agencies on the conduct of privacy impact assessments;
- b. oversee the implementation of the privacy impact assessment process throughout the Government; and
- c. require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

C. PRIVACY PROTECTIONS ON AGENCY WEBSITES. —

1. PRIVACY POLICIES ON WEBSITES. —

- a. GUIDELINES FOR NOTICES. —The Director shall develop guidance for privacy notices on agency websites used by the public.
- b. CONTENTS. —The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—
 - i. what information is to be collected;
 - ii. why the information is being collected;
 - iii. the intended use of the agency of the information;
 - iv. with whom the information will be shared;
 - v. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
 - vi. how the information will be secured; and
 - vii. the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the `Privacy Act'), and other laws relevant to the protection of the privacy of an individual.

2. PRIVACY POLICIES IN MACHINE-READABLE FORMATS. — The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

D. DEFINITION. —In this section, 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.

Attachment C

This attachment is a summary by the Federal Trade Commission of its guidance regarding federal agency compliance with the Children's Online Privacy Protection Act (COPPA).

The hallmarks of COPPA for purposes of federal online activity are (i) notice of information collection practices (ii) verifiable parental consent and (iii) access, as generally outlined below:

- Notice of Information Collection Practices

Agencies whose Internet sites offer a separate children's area and collect personal information from them must post a clear and prominent link to its Internet privacy policy on the home page of the children's area and at each area where it collects personal information from children. The privacy policy should provide the name and contact information of the agency representative required to respond to parental inquiries about the site. Importantly, the privacy policy should inform parents about the kinds of information collected from children, how the information is collected (directly, or through cookies), how the information is used, and procedures for reviewing/deleting the information obtained from children.

In addition, the privacy policy should inform parents that only the minimum information necessary for participation in the activity is collected from the child. In addition to providing notice by posting a privacy policy, notice of an Internet site's information collection practices must be sent directly to a parent when a site is requesting parental consent to collection personal information from a child. This direct notice should tell parents that the site would like to collect personal information from their child, that their consent is required for this collection, and how consent can be provided. The notice should also contain the information set forth in the site's privacy policy, or provide an explanatory link to the privacy policy.

- Verifiable Parental Consent

With limited exceptions, agencies must obtain parental consent before collecting any personal information from children under the age of 13. If agencies are using the personal information for their internal use only, they may obtain parental consent through an e-mail message from the parent, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, agencies might seek confirmation from a parent in a delayed confirmatory e-mail, or confirm the parent's consent by letter or phone call²³.

However, if agencies disclose the personal information to third parties or the public (through chat rooms or message boards), only the most reliable methods of obtaining consent must be used. These methods include: (i) obtaining a signed form from the parent via postal mail or facsimile, (ii) accepting and verifying a credit card number in connection with a transaction, (iii) taking calls from parents through a toll-free telephone

number staffed by trained personnel, or (iv) email accompanied by digital signature.

Although COPPA anticipates that private sector Internet operators may share collected information with third parties (for marketing or other commercial purposes) and with the public (through chat rooms or message boards), as a general principle, federal agencies collect information from children only for purposes of the immediate online activity or other, disclosed, internal agency use. (Internal agency use of collected information would include release to others who use it solely to provide support for the internal operations of the site or service, including technical support and order fulfillment.) By analogy to COPPA and consistent with the Privacy Act, agencies may not use information collected from children in any manner not initially disclosed and for which explicit parental consent has not been obtained. Agencies' Internet privacy policies should reflect these disclosure and consent principles.

COPPA's implementing regulations include several exceptions to the requirement to obtain advance parental consent where the Internet operator (here, the agency) collects a child's email address for the following purposes: (i) to provide notice and seek consent, (ii) to respond to a one-time request from a child before deleting it, (iii) to respond more than once to a specific request, e.g., for a subscription to a newsletter, as long as the parent is notified of, and has the opportunity to terminate a continuing series of communications, (iv) to protect the safety of a child, so long as the parent is notified and given the opportunity to prevent further use of the information, and (v) to protect the security or liability of the site or to respond to law enforcement if necessary.

Agencies should send a new notice and request for consent to parents any time the agency makes material changes in the collection or use of information to which the parent had previously agreed. Agencies should also make clear to parents that they may revoke their consent, refuse to allow further use or collection of the child's personal information and direct the agency to delete the information at any time.

- Access

At a parent's request, agencies must disclose the general kinds of personal information they collect online from children as well as the specific information collected from a child. Agencies must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information, e.g., obtaining signed hard copy of identification, accepting and verifying a credit card number, taking calls from parents on a toll-free line staffed by trained personnel, email accompanied by digital signature, or email accompanied by a PIN or password obtained through one of the verification methods above.

In adapting the provisions of COPPA to their Internet operations, agencies should consult the FTC's web site at <http://www.ftc.gov/privacy/privacyinitiatives/childrens.html> or call the COPPA compliance telephone line at (202) 326-3140.

Attachment D

Summary of Modifications to Prior Guidance

This Memorandum modifies prior guidance in the following ways:

* Internet Privacy Policies ([Memorandum 99-18](#)):

- must identify when tracking technology is used to personalize the interaction, and explain the purpose of the feature and the visitor's option to decline it.
- must clearly explain when information is maintained and retrieved by personal identifier in a Privacy Act system of records; must provide (or link to) a Privacy Act statement (which may be subsumed within agency's Internet privacy policy) where Privacy Act information is solicited.
- should clearly explain an individual's rights under the Privacy Act if solicited information is to be maintained in a Privacy Act system of records; information about rights under the Privacy Act may be provided in the body of the web privacy policy or via link to the agency's published systems notice and Privacy Act regulation or other summary of rights under the Privacy Act (notice and explanation of rights under other privacy laws should be handled in the same manner).
- when a Privacy Act Statement is not required, must link to the agency's Internet privacy policy explaining the purpose of the collection and use of the information (point-of-collection notice at agency option).

- must clearly explain where the user may consent to the collection or sharing of information and must notify users of any available mechanism to grant consent.
- agencies must undertake to make their Internet privacy policies “readable” by privacy protection technology and report to OMB their progress in that effort.
- must adhere to the regulatory requirements of the Children’s Online Privacy Protection Act (COPPA) when collecting information electronically from children under age 13.

*Tracking Technology ([Memorandum 00-13](#)):

- prohibition against tracking visitors’ Internet use extended to include tracking by any means (previous guidance addressed only “persistent cookies”).? authority to waive the prohibition on tracking in appropriate circumstances may be retained by the head of an agency, or may be delegated to (i) senior official(s) reporting directly to the agency head, or to (ii) the heads of sub-agencies.? agencies must report the use of tracking technology to OMB, identifying the circumstances, safeguards and approving official.
- agencies using customizing technology must explain the use, voluntary nature of and the safeguards applicable to the customizing device in the Internet privacy policy.
- agency heads or their designees may approve the use of persistent tracking technology to customize Internet interactions with the government.

* Privacy responsibilities ([Memorandum 99-05](#))

- agencies to identify individuals with day-to-day responsibility for implementing the privacy provisions of the E-Government Act, the Privacy Act and any other applicable statutory privacy regime.
- agencies to report to OMB the identities of senior official(s) primarily responsible for implementing and coordinating information technology/web policies and privacy policies.

1. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.
2. Information in identifiable form is defined in section 208(d) of the Act as “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.” Information “permitting the physical or online contacting of a specific individual” (see section 208(b)(1)(A)(ii)(II)) is the same as “information in identifiable form.”
3. Clinger-Cohen Act of 1996, 40 U.S.C. 11101(6).
4. Clinger-Cohen Act of 1996, 40 U.S.C. 11103.
5. In addition to these statutorily prescribed activities, the E-Government Act authorizes the Director of OMB to require agencies to conduct PIAs of existing electronic information systems or ongoing collections of information in identifiable form as the Director determines appropriate. (see section 208(b)(3)(C)).
6. Information in identifiable form about government personnel generally is protected by the Privacy Act of 1974. Nevertheless, OMB encourages agencies to conduct PIAs for these systems as appropriate.
7. Consistent with agency requirements under the Federal Information Security Management Act, agencies should: (i) affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured, (ii) acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls, (iii) describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information, and (iv) provide a point of contact for any additional questions from users. Given the potential sensitivity of security-related information, agencies should ensure that the IT security official responsible for the security of the system and its information reviews the language before it is posted.
8. PIAs that comply with the statutory requirements and previous versions of this Memorandum are acceptable for agencies’ FY 2005 budget submissions.
9. Section 208(b)(1)(C).
10. See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.
11. Item 1 of the Supporting Statement reads: “Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information.”
12. Item 2 of the Supporting Statement reads: “Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information

- received from the current collection.”
13. Item 2 of the Supporting Statement reads: “Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.”
 14. Item 10 of the Supporting Statement reads: “Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.”
 15. Section 208(c)(1)(B)(v).
 16. Section 208(c)(1)(B)(vii).
 17. Section 208(c)(1)(B)(i-iv).
 18. When multiple Privacy Act Statements are incorporated in a web privacy policy, a point-of-collection link must connect to the Privacy Act Statement pertinent to the particular collection.
 19. Attachment C contains a general outline of COPPA’s regulatory requirements. Agencies should consult the Federal Trade Commission’s COPPA compliance telephone line at (202)-326-3140 or website for additional information at: <http://www.ftc.gov/privacy/privacyinitiatives/childrens.html>.
 20. Consistent with current practice, the agency head or designee may limit, as appropriate, notice and reporting of tracking activities that the agency has properly approved and which are used for authorized law enforcement, national security and/or homeland security purposes.
 21. Section 208(c)(1)(B)(vi).
 22. Federal Information Security Management Act of 2002 (Title III of P.L. 107-347), OMB’s related security guidance and policies (Appendix III to OMB Circular A-130, “Security of Federal Automated Information Resources”) and standards and guidelines development by the National Institute of Standards and Technologies.
 23. This standard was set to expire in April 2002, at which time the most verifiable methods of obtaining consent would have been required; however, in a Notice of Proposed Rulemaking, published in the Federal Register on October 31, 2001, the FTC has proposed that this standard be extended until April 2004. 66 Fed. Reg. 54963.

**IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION**

**JIM HENRY PERKINS and JESSIE FRANK
QUALLS, on their own behalf and on the
behalf of all others similarly situated,**

Plaintiffs,

v.

CV No. 2:07-310-IPJ

**UNITED STATES DEPARTMENT OF
VETERANS AFFAIRS; et al.**

Defendants.

MEMORANDUM OPINION

This case is before the court upon remand from the Eleventh Circuit to conduct a “claim-by-claim” analysis to determine the validity of plaintiffs’ remaining challenges brought under the Administrative Procedures Act (“APA”), 5 U.S.C. § 551 *et seq.*, and seeking to enforce provisions of the Privacy Act, 5 U.S.C. § 552a; the E-Government Act of 2002, 44 U.S.C. § 3501 note; and the Veterans Benefits, Health Care, and Information Technology Act of 2006, 38 U.S.C. § 5724. Only counts two, five, six, and eight remain, and the court examines each claim in turn.

Factual Background

On January 22, 2007, an employee of the U.S. Department of Veterans

Affairs (“VA”) reported an external hard drive containing personally identifiable information and individually identifiable health information of over 250,000 veterans was missing from the Birmingham, Alabama Medical Center’s Research Enhancement Award Program (“REAP”). VA Office of Inspector General (“OIG”) Report, at 7. The IT Specialist responsible for the external hard drive, “John Doe,” used the hard drive to back up data on his computer and other data from a shared network drive.¹ The hard drive is thought to contain the names, addresses, social security numbers (“SSN”), dates of birth, phone numbers, and medical files of hundreds of thousands of veterans and also information on more than 1.3 million medical providers. VA OIG Report at 7, 9 (doc. 33-2). To date, it has not been recovered.

John Doe was an IT Specialist working for the Birmingham REAP, a program that focused on “changing the practices of health care providers to ensure that they provide the latest evidence-based treatment, and on using VA databases

¹The REAP Director approved the purchase of external hard drives as a means to provide more space to the Medical Center’s near-full server. VA OIG Report, at 15. No policy required the protection of sensitive data on removable computer storage devices unless such devices were to be carried outside a VA facility. *Id.* at 16. The REAP Director claimed the Information Security Officer (“ISO”) conferred with him in making the decision to purchase the external hard drives, but the ISO claimed he was not involved and did not know of the need for additional server space. The VA OIG concluded no one made a timely request to the ISO for additional space. VA OIG Report, at 15.

to link the care of VA patients to more general information on the population as a whole.” *Id.* at 3. To reach these goals, the Birmingham REAP collects data on patients and medical providers from multiple sources for dozens of separate research projects.” *Id.* The Data Unit of the Birmingham REAP was comprised of the Data Unit Manager, three IT Specialists, and two student program support Assistants. *Id.* at 4. John Doe worked “with national VA databases and design[ed] statistical programs to support Birmingham REAP research projects.” *Id.*

The VA OIG identified three projects for which John Doe was conducting research. The first “involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure”; the second “involved examining the quality of care to patients following myocardial infarction . . . , and attempted to determine whether certain demographic characteristics of the medical providers, such as their age, impacted the care rendered to these patients”; and the third “involved using a patient survey to identify use of over-the-counter medications in patients taking prescription medications and link the information obtained to various VA databases to determine whether patients suffered any adverse effects from the combination of medications.” *Id.* at 22, 25, 30. In gathering the information needed to complete these projects, John Doe improperly received

access to various databases and stores of information, and various components of the VA improperly released information to John Doe or gave John Doe such access. *Id.* at 22-33. He was therefore able “to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of the projects he was working on. [The OIG] believe[s] much of this information was stored on the missing external hard drive.” *Id.* at 22. Accurate reporting of what information was on the external hard drive has been difficult because the hard drive is still missing; John Doe encrypted or deleted multiple files from his computer after reporting the data missing; and John Doe was not initially forthright with criminal investigators. *Id.* at ii.

After John Doe reported the missing hard drive on January 22, 2007, the VA Security Operations Center (“SOC”) was immediately notified. *Id.* at 7. The SOC wrote a report and provided it to the VA OIG on January 23, 2007; on that same day, an OIG criminal investigator came to the Birmingham VAMC and conducted an interview. The Federal Bureau of Investigation became involved in the investigation on January 24, 2007. A forensic analysis of John Doe’s computer began on January 29, 2007, and on February 1, 2007, the OIG began to analyze what data could have been on the missing hard drive. *Id.* at 8, 9. Press releases dated on February 2 and 10, 2007, discussed the loss of the hard drive and the information it contained.

Subsequent to the reported loss of the Birmingham REAP data but prior to receiving the results of the OIG analysis of this data on February 7, 2007, VA senior management concluded that anyone whose SSN was thought to be contained in any of the missing files, irrespective of the ability of anyone possessing this data to match an SSN with a name or any other personal identifier, should be notified and offered credit protection. The basis for this decision was a memorandum issued on November 7, 2006. . . . The memorandum states that “in the event of a data loss involving individual and personal information. . . VA officials have a responsibility to notify the individual(s) of the loss in a timely manner and to offer these protection services.”

Id. at 11. The VA sent letters to those individuals whose information was thought to be compromised by the data breach, which gave them the option of one year of free credit monitoring services. *Id.* at 12.

The VA had also requested the Department of Health and Human Services to perform a risk analysis focusing on the Centers for Medicaid and Medicare Services (“CMS”) data involved in the breach. *Id.* The missing external hard drive contained approximately 1.3 million health care providers’ information,

including the SSNs of 664,165 health care providers. *Id.* On March 28, 2007, the CMS Chief Information Officer and Director sent a letter to the VA Assistant Secretary for Office of Information and Technology that stated, based on the CMS's completed independent risk analysis:

[T]here is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned. The letter requested that "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file."

Id. From April 17 to May 22, 2007, the VA sent notification letters to the 1.3 million health care providers. *Id.* By May 31, 2007, it sent additional letters offering one year of credit monitoring to the 664,165 health care providers whose SSNs appeared to be on the hard drive. VA OIG Report, at 12.

Analysis

A valid claim under the APA must attack agency action, which is defined as "includ[ing] the whole or a part of an agency rule, order, license, sanction, relief or the equivalent or denial thereof, or failure to act." *Fanin v. U.S. Dep't of*

Veterans Aff., 572 F.3d 868, 877 (11th Cir. 2009) (citing 5 U.S.C. § 551(13)).

If the claim attacks an agency’s action, instead of failure to act, and the statute allegedly violated does not provide a private right of action, then the “agency action” must also be a “final agency action.” [5 U.S.C. § 704; *see also Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 61-62, 124 S.Ct. 2373, 2379 (2004)]. “To be considered ‘final,’ an agency’s action: (1) must mark the consummation of the agency’s decisionmaking process—it must not be of a merely tentative or interlocutory nature; and (2) must be one by which rights or obligations have been determined, or from which legal consequences will flow. *U.S. Steel Corp. v. Astrue*, 495 F.3d 1272, 1280 (11th Cir. 2007)(quoting *Bennett v. Spear*, 520 U.S. 154, 177-78, 117 S.Ct. 1154, 1168 (1997)).

Id. However, if the claim challenges a failure to act, the court may compel “agency action unlawfully withheld or unreasonably delayed. . . only where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required* to take.” *Id.* at 877-878 (citing *Norton*, 542 U.S. at 64) (emphasis in original).

Further, the court notes the remaining claims seek only injunctive and

declaratory relief. Such relief may be granted only if the plaintiffs demonstrate that they are “likely to suffer future injury.” *City of Los Angeles v. Lyons*, 461 U.S. 95, 105, 103 S.Ct. 1660, 1667 (1983); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564, 112 S.Ct. 2130, 2138 (1992) (citing *Lyons*, 461 U.S. at 102) (“Past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief.”); *Seigel v. LePore*, 234 F.3d 1163, 1176-77 (11th Cir. 2000) (*en banc*) (“As we have emphasized on many occasions, the asserted irreparable injury “must be neither remote nor speculative, but actual and imminent.”) (citations omitted). *Emory v. Peeler*, 756 F.2d 1547, 1552 (11th Cir. 1985) (To grant declaratory relief, “there must be a substantial continuing controversy between parties having adverse legal interests. The plaintiff must allege facts from which the continuation of the dispute may be reasonably inferred. Additionally, the continuing controversy . . . must be real and immediate, and create a definite, rather than speculative threat of future injury.”).

Count Two

The plaintiffs claim that the VA failed “to create and maintain an accounting of the date, nature, and purpose of its disclosures” pursuant to the Privacy Act, 5 U.S.C. § 552a(c)(1), when John Doe accessed VA files to complete

VA projects. Joint Status Report (“JSR”), at 8 (doc. 56). The Privacy Act requires [e]ach agency, with respect to each system of records under its control, shall–

(1) except for disclosures made under subsections (b)(1) or

(b)(2) of this section, keep an accurate accounting of–

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made. . .

5 U.S.C. § 552a(c)(1). Under the exception provided in subsection (b)(1), agencies need not provide an accounting for disclosures made to “officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.” 5 U.S.C. § 552a(b)(1). Accordingly, to the extent John Doe needed the information that he accessed to perform his duties, the VA had no obligation to account.

To the extent John Doe had no need for the information contained on the external hard drive in the performance of his duties, the plaintiffs must show the disclosure was pursuant to one of the provisions in 5 U.S.C. § 552a(b)(3)-(12).

See 5 U.S.C. § 552a(c)(1)(A). After failing to argue in the JSR that any of those subsections apply, plaintiffs now claim that the VA's disclosure to John Doe falls under 5 U.S.C. § 552a(b)(5), which requires accounting when the disclosure is "to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable."

However, the accounting requirement in 5 U.S.C. § 552a(b)(5) is not triggered by the activity at issue in this case. An accounting is required only upon a disclosure to a recipient described in that subsection. Although "recipient" is not defined in the Privacy Act, it does not stand to reason that an agency that maintains records needed by one of its own researchers to fulfill his duties would be required to provide *itself* with "advance adequate written assurance that the record will be used solely as a statistical research or reporting record." Indeed, pertinent legislative history and Office of Management and Budget ("OMB") regulations suggest that an accounting was only intended when the disclosures were to individuals or agencies outside the agency maintaining the record. See S. REP. NO. 93-1183 (1974) *reprinted in* U.S. CODE CONGRESSIONAL AND ADMINISTRATIVE NEWS, 6916, 6967 (stating that subsection 201(b)(4) "[r]equires any federal agency that maintains a personal information system or file to maintain an accurate accounting of the date, nature, and purpose of nonregular access

granted to the system, and each disclosure of personal information made to any person *outside the agency, or to another agency. . . .*) (emphasis added); H.R. No. 93-1416, 2 (describing the summary and purpose of the Act as “requir[ing] agencies to keep an accounting of transfers of personal records *to other agencies and outsiders*”); 40 Fed. Reg. 28955 (July 9, 1975) (differentiating between “agencies disclosing records” and “recipient agencies” in the context of 5 U.S.C. § 552a(b)(5)).

Even if subsection (b)(5) is applicable in this case, the plaintiffs argue only that John Doe gave an advance adequate written assurance before accessing information from only one database, the Veterans Integrated Service Network (“VISN”) 7 Data Warehouse. Plaintiff’s Response (doc. 64) at 4. Accordingly, subsection (b)(5) applies only for John Doe’s access to the VISN 7 Data Warehouse to perform research for “Project 1,” which involved diabetes management research. *See* VA OIG Report, at 22. Moreover, the plaintiffs cannot show that any failure to account for John Doe’s access to the VISN 7 Data Warehouse to research diabetes management is causing them harm. Although the plaintiffs are upset about the loss of their personal information and the prospect of potential credit fraud in the future, any accompanying harm is attributable to the

loss of the information in the first place, *not* the purported failure to account.² Thus, even assuming *arguendo* that 5 U.S.C. § 552a(b)(5) applies, the plaintiffs cannot show that the alleged harm is fairly traceable to the VA's conduct, a deficiency fatal to their claim. *See Allen v. Wright*, 468 U.S. 737, 753 & n.19, 104 S.Ct. 3315, 3325 & n.19 (1984) (plaintiffs do not have standing where they failed to allege injuries that are caused by the defendants).

Because of these sufficient and independent reasons, the plaintiffs have not shown that the VA failed to take discrete agency action that it was required to take. Accordingly, the court finds that the plaintiffs have failed to state a claim upon which relief can be granted, and Count Two is due to be **DISMISSED**.

²The plaintiffs urge, "The Veterans have a right to know what information [was on the hard drive]. They deserve to know the 'purpose' for which John Doe was using the information," Plaintiff's Response, at 8 (doc. 64). However, the VA OIG report details, to the extent determinable, the information on the hard drive and the purpose for which John Doe was accessing the information. The VA OIG Report states that the hard drive is believed to contain "personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the [CMS], on over 1.3 million medical providers." VA OIG Report, at i. Moreover, it was difficult for the VA to make such a determination, as John Doe was not candid when he was interviewed; he deleted or encrypted files from his computer after the hard drive went missing; and he tried to hide the extent, magnitude, and impact of the missing data. *Id.* at ii. Lastly, the plaintiffs know that the purpose John Doe was accessing the VISN 7 Data Warehouse was related to his research for "Project 1," *id.* at 22-23, which "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure," VA OIG Report, at 22.

Count Five

Count Five involves the VA’s alleged failure to establish appropriate safeguards in violation of the Privacy Act, 5 U.S.C. § 552a(e)(10). The plaintiffs have failed to argue that the alleged conduct of the VA constituted a failure of discrete agency action that the VA was required to take, but request that Count Five “move forward as detailed in the Plaintiffs’ Statement in the Joint Report.” Plaintiff’s Brief, at 13 (doc. 64). In the Joint Status Report, the plaintiffs devote just over one page to briefing this issue and cite 5 U.S.C. § 552a(e)(10),³ arguing that the VA failed to enforce this subsection in the numerous ways listed in their complaint.⁴ Joint Status Report (“JSR”), at 10-11 (doc. 56). The plaintiffs then

³5 U.S.C. § 552a(e)(10) requires the VA to “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”

⁴Plaintiffs cite specifically to paragraph 80 of the Second Amended Complaint (doc. 21), which states:

Among other things, Defendants’ failures include operating a computer system or database from which an employee, including John Doe, can download or copy information, like the Personal Information and the Medical Information, onto the VA External Hard Drive without proper encryption and when not necessary to perform his or her duties; failing to conduct a data access inventory for John Doe and other VA employees and contractors with access to the VA’s office at the Pickwick Conference Center; failing to provide software that would require or enable encryption of data downloaded or copied

ask the court for an injunction forcing full implementation and compliance “with Handbook 6500 and other procedures and policies put in place in Birmingham by the VA in response to this incident, to conduct an independent audit of its compliance, and to file that audit with the court.” Plaintiff’s Response, at 14 (doc. 64) (footnotes added). Such an injunction is untenable.

Handbook 6500 is a seventy-one page (seven appendices excluded) document that details the responsibilities of almost two dozen information security personnel and dozens of policies and procedures. As pointed out by the defense, policies explained in the Handbook include maintaining the temperature in the building and proper use of the facsimile machines. In addition, the “other procedures and policies” put in place at the Birmingham facility are also

to mobile hard drives and devices, like the VA External Hard Drive from VA computers and databases at the VA offices and facilities in the Birmingham, Alabama area; failing to secure the VA External Hard Drive under lock and key when not in the immediate vicinity of John Doe; failing to house and protect the VA External Hard Drive to reduce the opportunities for unauthorized access, use, or removal; failing to provide intrusion detection systems at the VA office at the Pickwick Conference Center; failing to store the VA External Hard Drive in a secure area that requires proper escorting for access; failing to require and conduct appropriate background checks on all VA employees and contractors with access to the VA Office in the Pickwick Conference Center; and failing to protect against the alienation and relinquishment of control over the VA External Hard Drive, causing the Personal Information and Medical Information to be exposed to unidentified third parties.

Second Amended Complaint (doc. 21), ¶ 80.

numerous. *See e.g.*, VA Directive 6504 (doc. 61-3) (governing the transmission, transportation and use of, and access to, VA data outside VA facilities); VA Handbook 6500, at 7 (doc. 61-4) (a seventy-one page document “establish[ing] the foundation for VA’s comprehensive information security program and its practices that will protect the confidentiality, integrity, and availability of information”); Medical Center Memo 00-ISO-02 (doc. 61-5) (“assign[ing] responsibility and establish[ing] procedures for managing computer files at the Birmingham VA Medical Center”); Medical Center Memo 00-ISO-05 (doc. 61-6) (requiring VA employees at the Medical Center to get permission before use of removable storage media, especially Universal Serial Bus (“USB”) devices, and requiring written permission for the removal of sensitive information from VA facilities); Information Security Program VISN 7 AIS Operational Security Policy (doc. 61-9) (establishing procedures to implement a “structured program to safeguard all IT assets”); Memorandum 10N7-077 of VISN 7 VA Southeast Network (doc. 61-10) (stating “It is the policy of VISN 7 that no sensitive information ([personal health information or personal identifiable information]) will be stored on the storage media of any device without encryption or where the device is not *physically secured* to prevent accidental loss of sensitive information in the event of theft”) (emphasis in original).

Cases that suggest a broad injunction enforcing all of these policies is

appropriate are “relic[s] of a time when the federal judiciary thought that structural injunctions taking control of executive functions were sensible. That time has past.” *Rahman v. Chertoff*, 530 F.3d 622, 626 (7th Cir. 2008). “The limitation to discrete agency action precludes the kind of broad programmatic attack [the Supreme Court] rejected in *Lujan v. National Wildlife Federation*, 497 U.S. 871, 110 S.Ct 3177, 111 L.Ed.2d 695 (1990).” *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64, 124 S.Ct. 2373, 2379-2380 (2004); *see Lujan*, 497 U.S. at 891

When presented with similar circumstances in *Lujan*, the Supreme Court responded:

Respondent alleges that violation of the law is rampant within this program-failure to revise land plans in proper fashion, failure to submit certain recommendations to Congress, failure to consider multiple use, inordinate focus upon mineral exploitation, failure to provide required public notice, failure to provide adequate environmental impact statements. Perhaps so. But respondent cannot seek *wholesale* improvement of this program by court decree, rather than in the office of the Department or the halls of Congress, where programmatic improvements are normally made.

Lujan, 497 U.S. at 891. Courts are not empowered to compel “compliance with

broad statutory mandates,” *Norton*, 542 U.S. at 66-67, nor can they engage in general review of an agency’s day-to-day operations to ensure such compliance. *Id.*; *Lujan*, 497 U.S. at 899.

Even if this court could pass on such a generalized challenge, the court is convinced that Count Five is moot.

“‘[A] case is moot when the issues presented are no longer “live” or the parties lack a legally cognizable interest in the outcome.’” *County of Los Angeles v. Davis*, 440 U.S. 625, 631, 99 S.Ct. 1379, 59 L.Ed.2d 642 (1979) (quoting *Powell v. McCormack*, 395 U.S. 486, 496, 89 S.Ct. 1944, 23 L.Ed.2d 491 (1969)). The underlying concern is that, when the challenged conduct ceases such that “ ‘there is no reasonable expectation that the wrong will be repeated,’ ” *United States v. W.T. Grant Co.*, 345 U.S. 629, 633, 73 S.Ct. 894, 97 L.Ed. 1303 (1953), then it becomes impossible for the court to grant “ ‘any effectual relief whatever’ to [the] prevailing party,” *Church of Scientology of Cal. v. United States*, 506 U.S. 9, 12, 113 S.Ct. 447, 121 L.Ed.2d 313 (1992) (quoting *Mills v. Green*, 159 U.S. 651, 653, 16 S.Ct. 132, 40 L.Ed. 293 (1895)).

City of Erie v. Pap’s A.M., 529 U.S. 277, 287, 120 S.Ct. 1382, 1390 (2000).

Because the evidence submitted to the court shows that new security procedures and policies have been implemented and the deficiencies revealed in the VA OIG Report have been remedied, there is no “live” issue for which this court can grant effectual relief.

Count Six

In Count Six, the plaintiffs claim that the VA failed to perform a privacy impact assessment (“PIA”) pursuant to the E-Government Act of 2002 when it procured the external hard drives. Pursuant to the E-Government Act, agencies must perform a PIA before “developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form.” 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(1)(A)). The definition of “information technology” includes “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* 44 U.S.C. § 3501 note, § 201 (applying definitions from 44 U.S.C. §§ 3502, 3601); 44 U.S.C. § 3502(9) (applying the definition of 40 U.S.C. § 11101(6)). The disputed issue is whether the purchase of the external hard drives triggered the duty to perform a PIA.

The plaintiffs claim that the inclusion of “any equipment” in the definition of information technology brings the hard drives within the meaning of the term, thereby requiring the PIA. However, such an interpretation is implausible, as it would require government agencies that maintain personal information on individuals to conduct or update a PIA each time it purchases any computer, monitor, router, telephone, calculator, or other piece of equipment involved in a system that stores, analyzes, or manages the data. Rather, the purchase of several external hard drives, seems to be a “minor change[] to a system or collection that do[es] not create new privacy risks,” and therefore does not require a PIA. *See* M-03-22, Attachment A 2.B.3.g., Office and Management and Budget (“OMB”) Guidance Implementing the Privacy Provisions of the E-Government Act of 2002, at Section II.B.3.f (doc. 61-15) (hereinafter “M-03-22”).

Lending support to this interpretation is the fact that PIAs are required 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 veterans 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. *See* 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(2)(B)); M-03-22, at Section II.C.1.a. These types of inquiries are certainly appropriate and required when the VA initially

created the Birmingham VAMC system and began collecting data, but not where already collected and stored data is simply being transferred from a server to an external hard drive. The factors above are not relevant for such a transfer and a new PIA would not be informative of what information is being collected, the intended use of the information, or with whom the information would be shared. Under such circumstances, Congress surely did not intend a PIA to be performed.

To the extent the plaintiffs argue that security procedures were not followed or hardware security protocols were breached at the VA facility in Birmingham when the external hard drive went missing, such claims are not actionable under the E-Government Act of 2002. Rather, those arguments should have been pursued pursuant to the Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541 *et seq.*, a claim that the plaintiffs waived after not pursuing it on appeal. *Fanin v. U.S. Dep't of Veterans Affairs*, 572 F.3d 868, 876 n.1.

Count 8

The final count before the court involves the VA's alleged failure to perform an independent risk analysis ("IRA") to determine the risk presented by the loss of the hard drive pursuant to the Veterans Benefits, Health Care, and Information Technology Act of 2006 (VBHCITA), 38 U.S.C. § 5724(a)(1). The plaintiffs also claim that the VA acted unreasonably by providing only one year of credit monitoring services.

The VBHCITA⁵ provides:

In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity or the Office of Inspector General of the Department conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

38 U.S.C. § 5724(a)(1).

After John Doe reported the missing hard drive on January 22, 2007, the VA launched an immediate investigation that culminated in the decision to offer one year of free credit monitoring services for 198,760 living individuals whose information was contained on the hard drive. VA OIG Report, at 12. The VA made this decision *before* the completion of the IRA conducted by the Centers for Medicaid & Medicare Services (“CMS”). On February 7, 2007, VA senior

⁵The VBHCITA became effective December 22, 2006. The data breach incident at issue occurred on January 22, 2007. The VA passed regulations that became effective June 22, 2007, six months after the passage of the VBHCITA and five months after the loss of the external hard drive.

management decided that anyone whose SSN was on the hard drive should be notified and offered credit protection. *Id.* at 11. Approximately one and one-half months later, on March 28, 2007, the CMS Chief Information Officer and Director stated that based on the IRA, “There is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned.” *Id.* at 12. He recommended that the “VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file.” *Id.* Notification letters were sent out to the health care providers by May 31, 2007. *Id.*

Thus, the VA proactively assumed that the veterans were at risk and provided the remedy provided in the statute⁶ *before* it had confirmation from the IRA that such a remedy was appropriate under the circumstances. By presuming a reasonable risk of harm from the disclosure of personally identifiable information and providing credit protection services required when an IRA reveals a “reasonable risk” of harm, *see* 38 U.S.C. § 5724(a)(2), the VA has provided the

⁶In addition, VA regulations limit credit monitoring awarded to those who are subject to a reasonable risk for misuse of sensitive personal information to one year. 38 C.F.R. § 75.118(a).

plaintiffs with any relief they are due.⁷ Indeed, the IRA conducted by CMS affirmed the propriety of the relief offered by the VA.

Despite having been given such relief, the plaintiffs insist the IRA was insufficient and urge an additional IRA focusing on the veterans must be completed. However, the statute does not require an *individual* risk analysis as the plaintiffs state in their JSR, *See* JSR, at 12-13, 15, only an *independent* risk analysis.⁸ The VA OIG Report contains multiple groups of individuals whose private information was compromised: veterans, VA OIG Report, at 7; physicians, *id.* at 10; deceased physicians, *id.*; other health care providers, *id.*; non-veteran, non-VA employees, *id.* at 24; and VA employees, *id.* Furthermore, some veterans were only identified by their SSNs; others were identified by SSNs and dates of birth; others by their name, SSN, and medical information; and others identified

⁷ The plaintiffs offer a General Accountability Office report that states that a May 5, 2006, incident involving a missing tape with sensitive information of thousands of individuals on it warranted “credit protection and data breach analysis for 2 years.” JSR, at 14. As the plaintiffs explain, however, only one year of credit protection was offered, while two years of breach analysis was given. Declaration of Michael Hogan (“Hogan Decl.”), ¶¶ 2 (doc. 61-19) and Attachment A (doc. 61-20).

⁸The plaintiffs’ argument that the CMS was an inappropriate entity to perform the IRA has no merit, as the statute requires either the VA OIG or a non-Department [of Veterans Affairs] entity to conduct the IRA. 38 U.S.C. § 5724(a)(1). The CMS is under the purview of the Department of Health and Human Services.

by various combinations of seven fields of identifying information. *Id.* at 9. The health care providers are identified on the hard drive by different combinations of forty-eight different fields of data. *Id.* at 10. All of this information was on a single external hard drive lost during a single data breach. The statute only requires an “independent risk analysis of the data breach,” not multiple IRAs for each group of individuals whose information was compromised. *See* 38 U.S.C. § 5724(a)(1).

Because the plaintiffs were awarded appropriate relief and because the VA conducted an adequate IRA of the data breach, the court finds that the VA did not fail to take agency action it was required to take with respect to count eight.

Conclusion

Having considered the foregoing and being of the opinion that the plaintiffs have failed to properly state any claims challenging final agency action under the Administrative Procedures Act, 5 U.S.C. § 551 *et seq.*, the court finds that Counts Two, Five, Six, and Eight shall be **DISMISSED**. The court shall so rule by separate order.

DONE and ORDERED, this the 21st day of April 2010.



INGE PRYTZ JOHNSON
U.S. DISTRICT JUDGE

Interstate Voter Registration Crosscheck Program

National Association of
State Election Directors

January 26, 2013

JA000185



Kris W. Kobach

National Voter Registration Act of 1993

- **Section 2 Findings and Purposes**
- (b) Purposes
 - (1) to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office;
 - (2) to make it possible for Federal, State, and local governments to implement this subchapter in a manner that enhances the participation of eligible citizens as voters in elections for Federal office;
 - (3) to protect the integrity of the electoral process; and
 - **(4) to ensure that accurate and current voter registration rolls are maintained.**

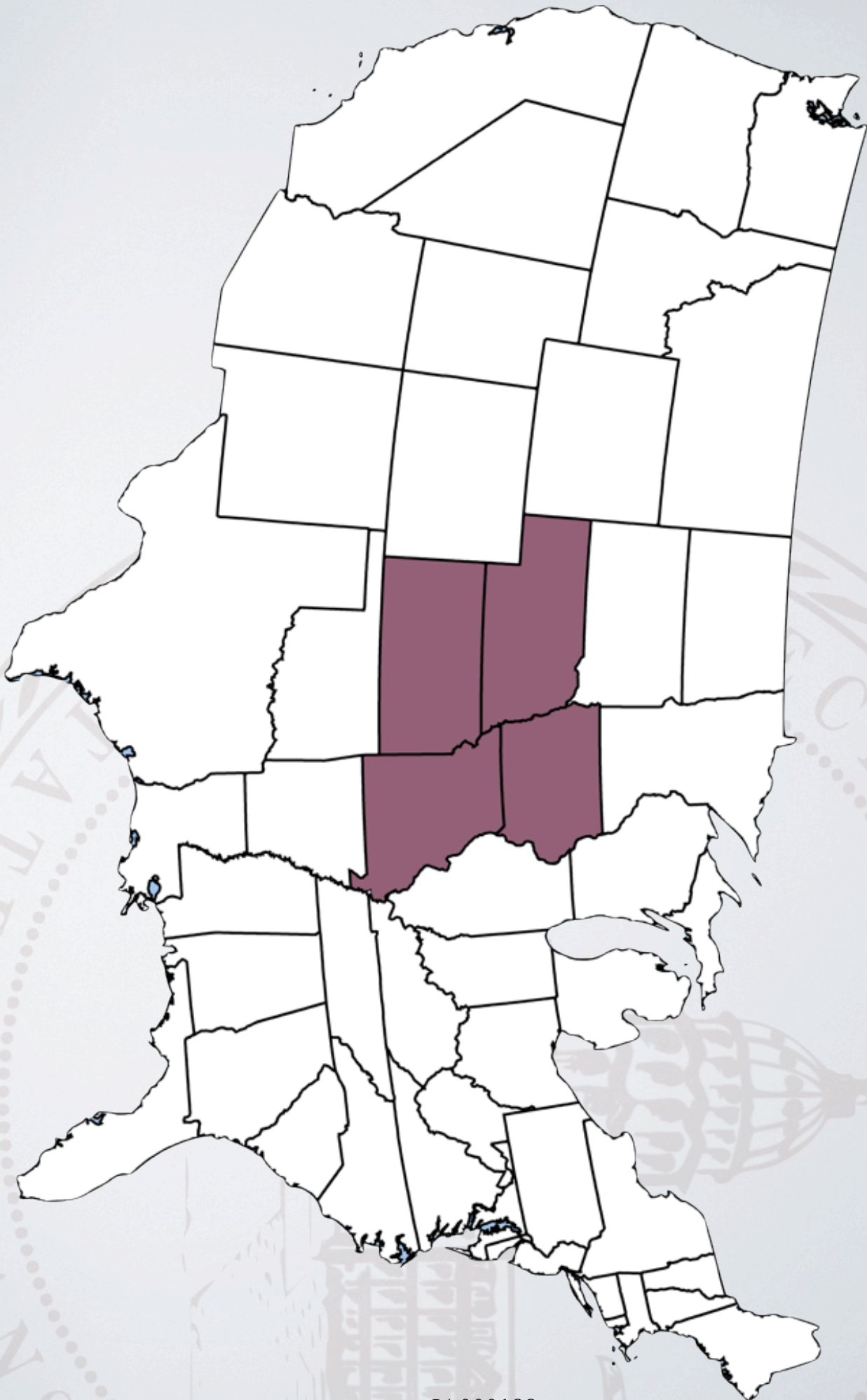
JA000186



From the Federal Election Commission's guide: Implementing the National Voter Registration Act of 1993:

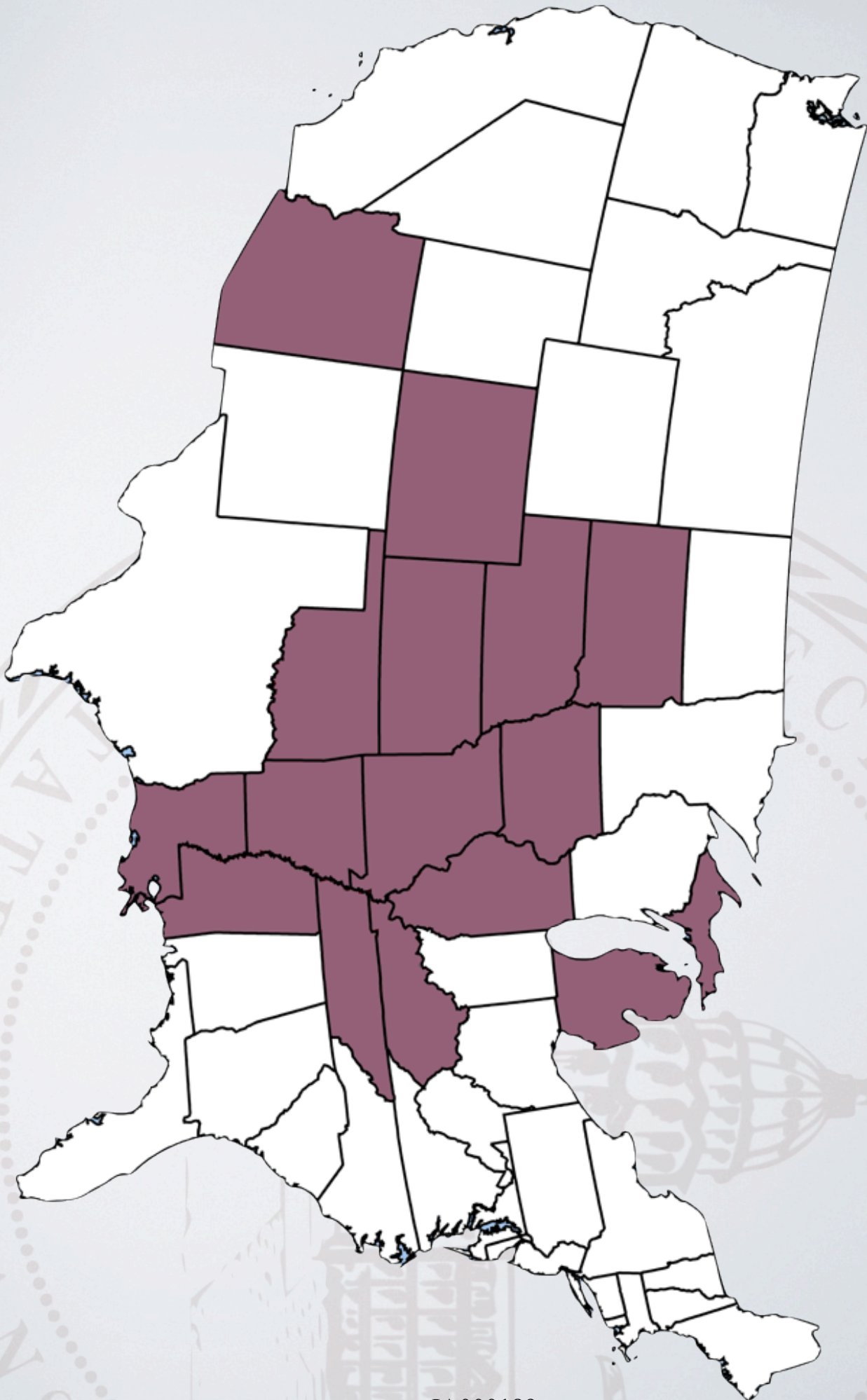
The features (of the National Voter Registration Act) include a requirement that states “conduct a general program” the purpose of which is “to protect the integrity of the electoral process by ensuring the maintenance of an accurate and current voter registration roll for elections for Federal office”

Participants in 2005

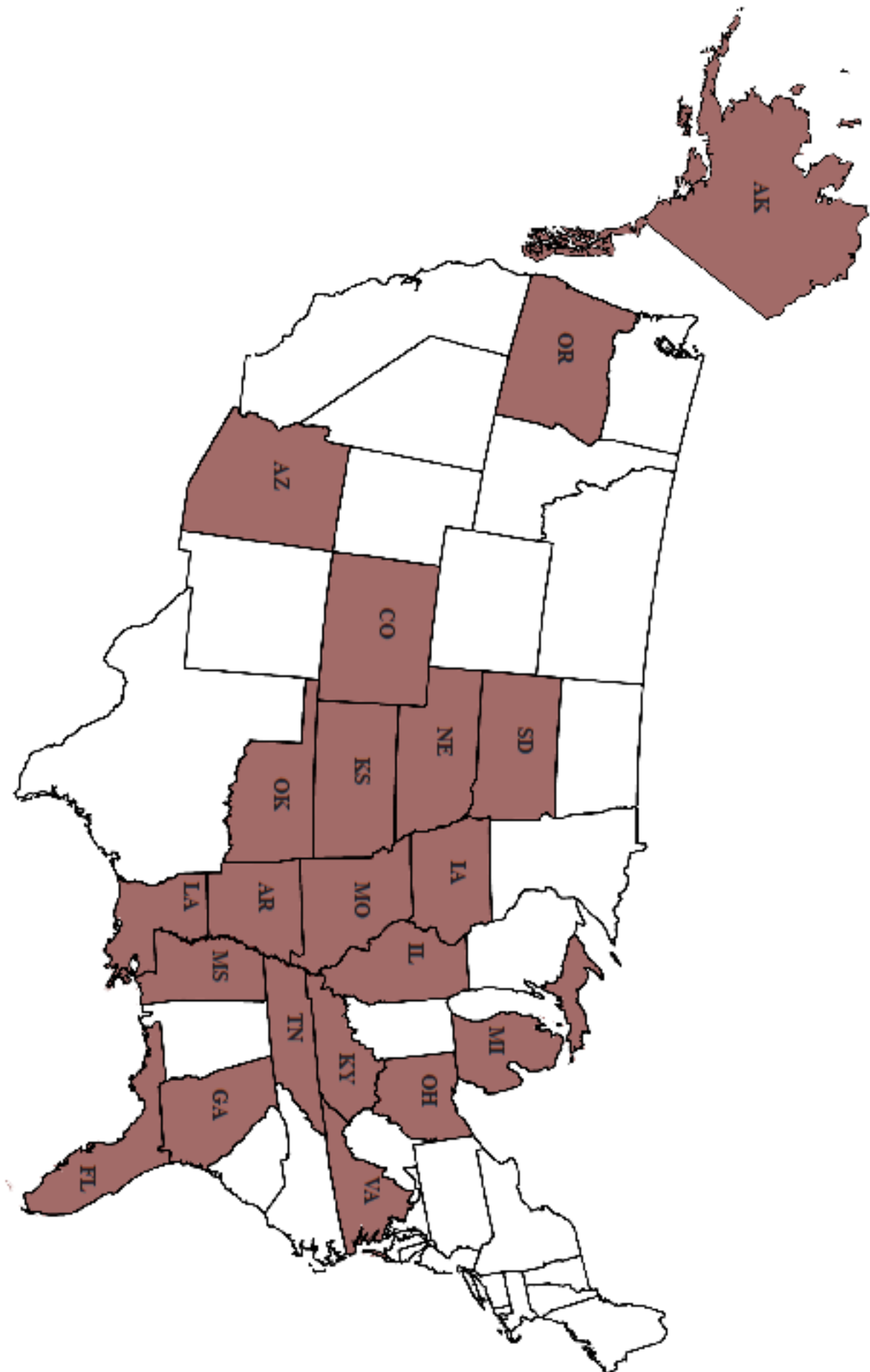


JA000188

Participants in 2012



JA000189



JA000190

2013 Interstate Crosscheck

Participating states as of Jan. 10, 2013

2012 Crosscheck Program—Number of Records Compared

Arizona	3,545,891	Michigan	7,337,846
Arkansas	1,528,458	Mississippi	2,002,406
Colorado	3,375,891	Missouri	4,069,576
Illinois	8,248,736	Nebraska	1,129,943
Iowa	2,113,199	Oklahoma	2,000,767
Kansas	1,702,495	South Dakota	560,147
Kentucky	1,303,684	Tennessee	3,468,503
Louisiana	2,860,281		

Total Records: 45,247,823

Interstate Crosscheck Data Format

Field	Format	Example
Status	A=Active; I=Inactive	A
Date_Generated	YYYY/MM/DD	2010/01/01
First_Name		Bob
Middle_Name		Alan
Last_Name		Jones
Suffix Name		Jr
Date_of_Birth	YYYY/MM/DD	1940/06/16
Voter_ID_Number		123456
Last_4_SSN		7890
Mailing Address	Line 1 Line 2 City State Zip	123 Anywhere St...
County		Allen
Date_of_Registration	YYYY/MM/DD	1970/01/01
Voted_in_2010	Y=did vote; N=did not vote	Y

JA000192



How does it work?

- Each state pulls data on January 15 each year using prescribed data format
- Upload data to secure FTP site (hosted by Arkansas)
- Kansas IT department pulls data, runs comparison, uploads results to FTP site
- Each state downloads results from FTP site, processes them according to state laws & regulations
- Kansas deletes all other states' data

JA000193





First: John
Middle: Q.
Last: Public
DOB: 01/01/1975
SSN: 1234
State: Kansas

First: John
Middle:
Last: Public
DOB: 01/01/1975
SSN: 1234
State: Colorado

Potential match



Grid of Potential Duplicate Voters Within States															
Case: 17-cv-01328-CKR Document 33-2 Filed 07/13/19 Page 73 of 119															
		by DOB Last Name First Name													
2012	AZ	AR	CO	IL	IA	KS	KY	LA	MI	MS	MO	NE	OK	SD	TN
AZ		2,829	24,863	16,014	7,153	3,687	688	2,062	27,617	2,220	7,569	3,306	4,006	2,449	3,614
AR	2,829		4,557	6,950	2,430	2,686	691	5,957	5,085	6,477	11,049	995	7,403	433	7,180
CO	24,863	4,557		19,902	10,850	10,035	1,054	5,065	17,086	3,309	12,498	8,927	8,306	3,937	6,153
IL	16,014	6,950	19,902		10,850	10,035	1,054	5,065	17,086	3,309	12,498	8,927	8,306	3,937	6,153
IA	7,153	2,430	10,850	31,882		4,706	526	1,558	7,019	1,797	11,563	3,803	2,031	4,865	2,806
KS	3,687	2,686	10,035	6,311	4,706		401	1,369	4,461	1,397	31,082	4,196	6,575	905	2,205
KY	688	691	1,054	2,467	526	401		873	2,267	1,085	1,995	576	6,575	117	1,905
LA	2,062	5,957	5,065	5,207	1,558	1,369	873		6,851	17,744	5,254	2,829	2,829	277	4,422
MI	27,617	5,085	17,086	49,260	7,019	4,461	2,267	6,851		7,527	12,960	2,416	4,067	1,265	16,956
MS	2,220	6,477	3,309	10,766	1,797	1,397	1,085	7,527	7,527		5,607	780	2,364	305	21,661
MO	7,569	11,049	12,498	39,658	11,563	31,082	1,195	5,254	12,960	5,607		4,244	7,539	1,300	7,804
NE	3,306	995	8,927	3,803	10,954	4,196	233	810	2,416	780	4,244		1,126	2,608	1,108
OK	4,006	7,403	8,306	4,834	2,031	6,575	576	2,829	4,067	2,364	7,539	1,126		402	2,858
SD	2,449	433	3,937	1,500	4,865	905	117	277	1,265	305	1,300	2,608	402		537
TN	3,614	7,180	6,153	12,469	2,806	2,205	1,905	4,422	16,956	21,661	7,804	1,108	2,858	537	
Totals	108,077	64,722	136,542	211,023	100,140	80,016	14,078	60,278	164,837	83,039	159,322	45,506	54,916	20,900	91,678

Success in Kansas

Double Votes from 2008 and 2010 Referred to Prosecution Discovered through Interstate Crosscheck Program

2008	2010
Kansas - Kentucky	Kansas – Arkansas (2)
Kansas - Colorado	Kansas – Colorado (5)
Kansas - Kansas	Kansas – Iowa
	Kansas – Louisiana
	Kansas – Nebraska
	Kansas - Oklahoma



Success in other states - Colorado


- Four individuals indicted for voting in Colorado and Arizona in first year of participation
- Six additional cases of double voting referred to FBI in 2012



Kris W. Kobach

STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80230

FOR IMMEDIATE RELEASE
January 23, 2012



News Release

**Cross-state voter comparison identifies double voters
CO and KS identify individuals who voted twice in 2010 election**

Denver, Colorado - Secretary of State Scott Gessler today announced his office referred information to the FBI regarding individuals suspected of voting twice during the 2010 election. Following a comparison of voting records between Kansas and Colorado, six voters appear to have cast ballots in both states.

Voter fraud undermines our electoral system. Secretary Gessler said, "I will continue to be vigilant and undertake these kinds of anti-fraud measures. These state crosschecks are an important component in ensuring the integrity of our election process."

Since 2008, Colorado has shared voter records with a consortium of states to monitor and undertake these kinds of anti-fraud measures. The Colorado Secretary of State's office turned over information to the FBI that matched individual voter records including date of birth and signature on ballots cast in both Colorado and Arizona. Now, following the 2010 election, the investigation has referred to FBI in 2012. Persons convicted of voter fraud in Colorado can be sentenced to three years in prison and fines in excess of \$1,000.

###

Media Contacts: Rich Coolidge
richard.coolidge@sos.state.co.us Andrew Cole
andrew.cole@sos.state.co.us (303) 860-6303

Scott Gessler
Secretary of State
William A. Hobbs
Deputy Secretary of State

JA000197

What does it cost to participate?

\$0

JA000198



Kris W. Kobach

How Can a State Join the Crosscheck?

1. Chief State Election Official signs the Memorandum of Understanding (MOU)
2. CSEO assigns two staff members:
 - one election administration person
 - one IT person
3. Staff members will:
 - participate in annual conference call and email
 - pull VR data in January
 - receive cross check results and process
 - instruct local elections officials (respond to requests for addresses, signatures on poll books, etc.)

JA000199



Contact

Brad Bryant

State Election Director

Kansas Secretary of State's Office

brad.bryant@sos.ks.gov

785-296-4561

JA000200



canvassing kansas

Published by the Office
of the Secretary of State

EDITORS

Brad Bryant
Kay Curtis

LAYOUT AND DESIGN

Todd Caywood

CONTRIBUTORS

Brad Bryant
Kay Curtis

Suggestions or comments?
Please call (785) 368-8095.

This publication may be duplicated for informational purposes only. No written permission is required with the exception of articles or information attributed to a source other than the Kansas Secretary of State.

© 2013

Kansas Secretary of State
Memorial Hall
120 SW 10th Ave.
Topeka, KS 66612-1594
(785) 296-4564



From the desk of the Secretary

“Lead, follow, or get out of the way.”

Thomas Paine, 1737 - 1809. Kansas has consistently chosen the former when it comes to elections.

In 2005 Kansas took the lead when four states agreed to compare voter registration records with each other annually in order to identify duplicate voter registrations and double votes. Our IT department pulls data from a secure FTP site, runs comparisons and uploads the results to the FTP site on January 15 each year. Then each participating state can download its results and process them according to their own laws and regulations. The Interstate Voter Registration Crosscheck Program had increased to 14 participating states when I took office in 2011.

Convinced of the value of the program, I decided that I would make it one of my highest priorities to increase the number of participating states, hopefully doubling its size. The more states that participate, the more duplicate records each participating state can find. I contacted chief election officers in other states to explain how Crosscheck works and the value of this tool to maintain clean, current, and accurate voter lists to fight voter fraud. As a result, the number of states participating has more than doubled to 29 states that will share voter registration data in January 2014. While I am very pleased that over half of the 50 states are currently on board, I will continue to promote Crosscheck as an effective means of list maintenance.

In 2008 Kansas took the lead in helping voters to find election information when they need it by using internet search engines. As part of the Voting Information Project (VIP), Kansas contracted with ES&S to make programming changes to our ELVIS database so that all states with ES&S can provide a data feed to the VIP program which hosts the data. Google acknowledged our contribution by presenting a Kansas-shaped VIP award to the State of Kansas at the summer NASS conference.

Finally, in 2011 Kansas took the lead as the first state to combine three election-security policies: (1) requiring a government-issued photo ID for voting in person, (2) requiring either a Kansas driver’s license number or photocopy of a current photo ID for applying for a mail-in ballot, and (3) requiring a document proving U.S. citizenship when a person registers to vote for the first time. Consequently, Kansas elections are the most secure in the nation against fraud.

Thank you for all you have done to help implement these reforms. Together we have made Kansas the nation’s leader.

Voting Information Project Award Received at NASS

On July 19th, 2013, Google presented an award to recognize Kansas' efforts to improve the efficiency and effectiveness of elections through open data. Eight other states also received the award at the National Association of Secretaries of State 2013 Summer Conference in Anchorage, Alaska. Each of the nine states had participated in the Voting Information Project (VIP) by publishing polling places and other election data as part of the open data effort. Secretary of State Kris Kobach was present to accept the award for his office.

By joining the project on the ground floor, Kansas was among the first states to help registered voters to more readily find election information when they need it and where they are most likely to look for it. Government websites often are not the first place voters look. VIP is similar to the online VoterView feature of the Kansas voter registration system, and voters who perform Google searches for voter registration information will end up at the VoterView website as a result of the VIP.

In the run up to the 2012 general election, 22 million times users queried the Google Civic Information API. According to the VIP program, "When the project started in 2008, nobody involved knew whether the open data effort would have any impact at all. Early adopters took a risk on something new by agreeing to participate and the payoff was immense."

The VIP program was initiated as a cooperative effort between the Pew Foundation and Google. As a private charitable organization, Pew's rules do not allow them to pay money to a private for-profit corporation, so Pew asked the Kansas SOS office to serve as a go-between. The SOS office wrote specifications and requested Election Systems & Software to make the required programming changes in the voter registration database. The cost of the programming was paid by Pew to the SOS office and passed on to ES&S. As a result, all states with ES&S databases benefit from the new functionality.

For more information about Kansas participation in the VIP project since 2008, see *Canvassing Kansas*, September 2010, page 6. ■

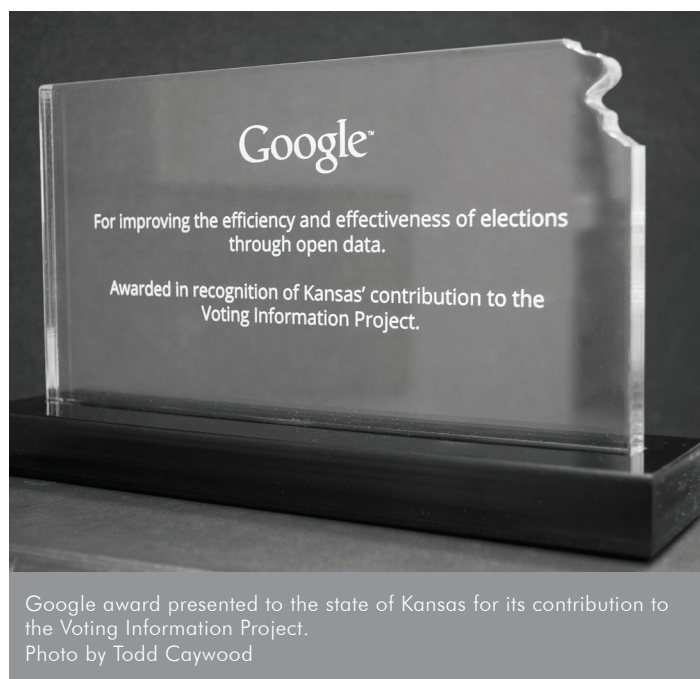
Clemens Receives CERA Certification

Cystal Clemens, Seward County Deputy Clerk/Election Officer, completed the Election Center's CERA program this year. Certificates were presented at the Election Center's annual national conference in Savannah, GA, held August 13-17, 2013. Crystal was one of fifty eight election officials to receive the award this year.

CERA (Certified Elections/Registration Administrator) is one of very few nationally recognized programs providing professional training for election administrators. The Election Center itself is a nationwide professional association of local, county and state voter registrars and election administrators that promotes training and best practices, monitors and lobbies on federal legislation, and provides a forum for the exchange of ideas.

Completion of the CERA program requires travel and attendance at a number of training sessions across the country over a period of years. Crystal is one of a small handful of Kansas election officials who have completed it.

Crystal's supervisor, Seward County Clerk Stacia Long, had this to say: "Crystal has always shown great passion for the entire election process. I am very proud of her designation as a CERA. She truly is a great asset to the Election Office and Seward County." ■



Google award presented to the state of Kansas for its contribution to the Voting Information Project.
Photo by Todd Caywood

Attorney General Issues Opinion on Concealed Carry

The office of Attorney General Derek Schmidt issued a formal opinion on November 27, 2013 in response to questions posed by Secretary of State Kris Kobach. Kobach requested the opinion in a letter dated September 30, 2013, as chief state election officer and on behalf of county election officers across the state.

The issue at the heart of the request was how polling places would be affected by passage of the Personal and Family Protection Act of 2013. The Act, passed as Senate Substitute for House Bill 2052 (2013 Kansas Session Laws, Chapter 105), authorizes persons who possess concealed carry permits to carry weapons into municipal buildings except under specific circumstances. "Municipal building" includes any facility owned or leased by a municipality, which could include facilities used as polling places during advance voting or on election day.

In his letter, Secretary Kobach asked the following questions:

- 1. Does the Act apply to privately-owned facilities used as polling places by verbal agreement?**
- 2. Does the Act apply to privately-owned facilities used as polling places by written agreement when no rent money is paid to the owner or manager of the site?**
- 3. Does the Act apply to privately-owned facilities used as polling places by written agreement when rent money is paid to the owner or manager of the site?**
- 4. If only one room or one portion of a building otherwise not subject to the Act is used as a polling place, does the Act apply to the entire building or only to the area used as a polling place?**
- 5. If an area in a nursing home, assisted living center or long term care facility is used for mobile advance voting pursuant to K.S.A. 25-2812, does the Act apply to the voting area?**
- 6. Do the provisions of the Act applicable to schools still apply to school facilities used as polling places?**

7. Is a county government liable for claims of denial of equal protection if various polling places have different levels of security as a result of implementation of the Act?

At the time of this writing, the secretary of state had just begun to analyze the opinion. The SOS office will communicate further information to CEOs when the analysis is complete. In the meantime, CEOs are encouraged to discuss the opinion with their county attorneys and counselors. The full opinion may be found online: <http://ksag.washburnlaw.edu/opinions/2013/2013-020.pdf>.

The synopsis from Attorney General Opinion 2013-20 is reproduced here:

Except as described herein, the use of real property as a polling place does not transform the nature of that property for the purposes of the PFPA. Any concealed carry requirements that applied to that property immediately before its temporary use as a polling place continue to apply during its use as a polling place and thereafter.

The Personal and Family Protection Act (PFPA) authorizes concealed carry licensees to carry a concealed handgun into a polling place to the extent that concealed handguns are permitted to be carried into the building in which the polling place is located.

The provisions of K.S.A. 2013 Supp. 75-7c20 apply only to buildings that are owned or leased in their entirety by the state or a municipality. If the PFPA requires concealed carry to be permitted in a state or municipal building, then concealed carry licensees must be permitted to carry a concealed handgun in all parts of the building, including areas used as polling places, with the exception of courtrooms, ancillary courtrooms, and secure areas of correctional facilities, jails and law enforcement agencies.

The governing body or chief administrative officer, if no governing body exists, of a state or municipal building may exempt the building from the provisions of K.S.A. 2013 Supp. 75-7c20 for a set period of time. If a state or municipal building is so exempted, concealed carry may be prohibited by posting the building in accordance with K.S.A. 2013 Supp. 75-7c10.

Cont'd on pg. 6

SOS Office Involved in Litigation

The office of the Kansas Secretary of State finds itself involved in three lawsuits that could affect the voter registration process and the 2014 elections. All are related to the 2011 Kansas SAFE Act. One case deals with the photo ID requirement and the other two deal with the requirement that new voters prove their U.S. citizenship the first time they register to vote.

1. *Arthur Sprye and Charles Hamner v. Kris W. Kobach*

In a suit filed November 1, 2013, two Osage County voters challenged the constitutionality of the photo ID requirement.

2. *Kris W. Kobach, Kansas Secretary of State; and Ken Bennett, Arizona Secretary of State; v. United States Election Assistance Commission*

In a suit filed in U.S. District Court in Kansas on August 21, 2013, the Kansas and Arizona Secretaries of State asked for a ruling to require the Election Assistance Commission to include the citizenship requirement in the voter instructions accompanying the universal federal voter registration application form, which is prescribed by the EAC. This lawsuit is in response to the June 17, 2013 ruling by the U.S. Supreme Court in *Arizona v. Inter Tribal Council of Arizona* regarding the constitutionality of states' requirements that voters provide proof

of citizenship. The Court's ruling indicated that states might file suit if the EAC declined to make the necessary changes to the voter registration form administratively.

3. *Aaron Belenky, Scott Jones, and Equality Kansas v. Kris Kobach, Kansas Secretary of State, and Brad Bryant, Kansas Elections Director*

In a suit filed November 21, 2013, the plaintiffs seek declaratory and injunctive relief to keep the secretary of state's office from implementing a dual voter registration system. The SOS office had developed contingency plans to administer voter registration and ballots to individuals who attempted to register using the universal federal form but who had not provided proof of U.S. citizenship in compliance with Kansas law. No actions have been taken to implement the plan, and no federal elections have occurred in which federal-only ballots were administered to these voters. (See also *Canvassing Kansas*, September 2013, page 1.)

The goal of the secretary of state's office is to have the cases decided as soon as possible so CEOs and poll workers will know the rules before preparations begin for the 2014 election season. ■

Kobach Reappoints Lehman

Secretary of State Kris Kobach reappointed Tabitha Lehman as Sedgwick County Election Commissioner in September 2013. Her regular term expires on July 19, 2017. This will be Lehman's first full term as election commissioner, having been appointed to fill an unexpired term in 2011.

Lehman was appointed in November 2011 to succeed Bill Gale who resigned his position to pursue other employment. Gale had been appointed in November 2003 to succeed Marilyn Chapman, and he was reappointed in July 2009.

Speaking of her reappointment, Lehman said:

"I appreciate the opportunity to continue serving the voters of Sedgwick County and look forward to providing them with safe and efficient elections in the coming four years." ■



Sedgwick County Election Commissioner Tabitha Lehman
Photo courtesy of Tabitha Lehman

Crosscheck

Cont'd

Evidence of double votes is presented to law enforcement officers for investigation and possible prosecution. The referral is usually made to county law enforcement officers, but state or federal officials may be involved in some cases.

States join the crosscheck by signing a Memorandum of Understanding. The chief state election officer (usually the secretary of state) or a designee may sign the MOU for a given state.

Participating states pull their entire voter registration databases and upload them to a secure FTP site on January 15 each year. The Kansas SOS office IT staff pull the states' data from the FTP site, run the comparison, and upload each state's results to the FTP site. Each state then pulls its results from the FTP site and processes them according to its individual laws, regulations and procedures. In Kansas, results are provided to CEOs with instructions for analyzing them and mailing confirmation notices.

The crosscheck program is one of several list maintenance programs used to keep registration records up to date. (See also *Canvassing Kansas*, March 2010, page 9.) ■

Attorney General

Cont'd

If the governing body or chief administrative officer of a state or municipal building does not exempt a building from the provisions of K.S.A. 2013 Supp. 75-7c20, then concealed carry licensees must be permitted to carry a concealed handgun inside the building unless adequate security measures are provided and the building is posted as prohibiting concealed carry.

Concealed carry is not required to be permitted in a polling place located inside a privately-owned building unless the county has leased the entire privately-owned building.

Concealed carry is not required to be permitted in polling places located inside public school district buildings because a public school district is not a municipality for the purposes of the PFFA.

An equal protection claim against a county based upon the varying ability of concealed carry licensees to carry a concealed handgun into a polling place would be subject to the rational basis test. ■

Jury List Program Initiated

A 2013 law which went into effect July 1, 2013, requires district courts in Kansas to provide to the secretary of state the names of prospective jurors who indicate on their jury questionnaires that they are not United States citizens. Noncitizens are exempt from jury duty. The secretary of state passes the names on to CEOs for review. If they are found to be registered voters, their registrations are canceled. (See 2013 House Bill 2164; 2013 Kansas Session Laws Chapter 85.)

The relevant section of the law is New Section 1, reproduced below. Most of the bill deals with grand juries.

New Section 1. (a) On and after July 1, 2013, any jury commissioner that receives information regarding citizenship from a prospective juror or court of this state that disqualifies or potentially disqualifies such prospective juror from jury service pursuant to K.S.A. 43-156, and amendments thereto, shall submit such information to the secretary of state in a form and manner approved by the secretary of state. Any such information provided by a jury commissioner to the secretary of state shall be limited to the information regarding citizenship and the full name, current and prior addresses, age and telephone number of the prospective juror; and, if available, the date of birth of the prospective juror. Any such information provided by a jury commissioner to the secretary of state shall be used for the purpose of maintaining voter registrations as required by law.

The secretary of state's office worked with the Office of Judicial Administration (OJA) to design the following procedure to comply with the law:

- The clerk in each of Kansas' 31 judicial districts will submit a monthly report directly to the SOS office containing names of persons who were exempted from jury duty on the basis of their claims to be non-U.S. citizens.
- Reports will be submitted via email on or after the 15th of each month beginning in December 2013.
- The SOS will notify OJA of missing reports. OJA will contact any such district court clerks to remind them to submit their reports.
- If any of the persons listed in the reports are found to be registered voters and their citizenship status is not in doubt, their names will be sent by the SOS office to the appropriate county election officers with instructions regarding the possible cancellation of the persons' voter registration records. ■

State Fair Opinion Poll Results

The Office of the Secretary of State has operated a booth in the Meadowlark Building at the Kansas State Fair in Hutchinson for more than 25 years. The dates of the fair this year were September 6-15. This was the 100th anniversary of the fair, and the theme was “Never Gets Old.”

At the booth, the SOS office provides information about agency activities, registers voters, and conducts an opinion poll on current issues. Don Merriman, Saline County Clerk, has assisted the SOS office for many years by lending ES&S iVotronic voting machines to help the fair visitors familiarize themselves with electronic voting technology. We want to recognize and thank Don for his assistance and the Lockwood Company for its donation of ballot programming services.

The SOS booth is mostly staffed by agency employees, but sometimes county election office personnel help out by volunteering to work in the booth. This year’s county volunteers were: Sharon Seibel, Ford County Clerk; Debbie Cox, Ford County Deputy Clerk; Donna Maskus, Ellis County Clerk; Don Merriman, Saline County Clerk; Crysta Torson, Lane County Clerk; and Karen Duncan, Lane County Deputy Clerk. Thanks to the volunteers for helping out!

Following are the results of the opinion poll:

Question #1: New Kansas voters must provide proof of citizenship when registering to vote.

- 709** *I approve of this requirement.*
96 *I do not approve of this requirement.*
27 *I have no opinion about this requirement.*

Question #2: Which university will advance the furthest in the 2014 NCAA Men’s Basketball Tournament?

- 397** *University of Kansas*
196 *Kansas State University*
179 *Wichita State University*
48 *None will make the tournament*

Question #3: Which of these alleged abuses of power by the federal government is the most concerning to you?

- 342** *NSA secretly collecting phone records of millions of U.S. citizens.*
332 *IRS intentionally discriminating against conservative organizations.*

153 *Presidential political appointees using secret email accounts to conduct official government business.*

132 *White House’s sweeping seizure of Associated Press records and cable television documents.*

Question #4: Should the Internal Revenue Service be abolished?

- 526** *Yes. A flat or fair tax is simpler, cheaper and easier to manage.*
86 *Yes. We shouldn’t have to pay income tax anyway.*
125 *No. Better training and oversight will fix most problems.*
2 *No. There is nothing wrong with the IRS.*

Question #5: Who is your favorite super hero?

- 90** *Xena: Warrior Princess*
379 *Superman*
94 *Wonder Woman*
195 *Batman* ■

Former Longtime Neosho County Clerk Dies

Wayne B. Gibson, Jr., a well known longtime county clerk from Neosho County, died on September 18, 2013, at a hospital in Labette County. Wayne served many years in the Neosho County Clerk’s office and was known to Kansas election officials as a hardworking, conscientious public servant.

Gibson started working in the county clerk’s office on January 16, 1961 and became Deputy Clerk about a month later. He then became Clerk on July 14, 1971, following the death of his predecessor, Virgil Lowe. Gibson served continuously until his retirement on April 20, 2007. During that time he was elected ten times - in 1972, 1974, 1976, 1980, 1984, 1988, 1992, 1996, 2000 and 2004.

The vacancy created by Gibson’s resignation was filled by Randal Neely, who took office on August 1, 2007, and continues in office today. ■

Dominion Seeks Voting System Certification

Dominion Voting Systems, Inc., submitted a letter dated October 4, 2013 requesting certification of its Democracy Suite Version 4.14 voting system. According to Kansas law, a manufacturer seeking certification of its voting system must submit a formal letter, pay a \$500 fee, and demonstrate the system at a certification hearing held in Topeka.

A hearing was held at the secretary of state's office on November 21, 2013, attended by Secretary of State Kris Kobach and members of his staff. The Democracy Suite system was demonstrated and explained by Norma Townsend, Don Vopalensky, Jeff Hintz and Michael Kelava. Dominion is represented in Kansas by its subcontractor, Election Source. Dominion also markets and services Premier (formerly Diebold) voting equipment, having purchased Premier from Election Systems and Software several years ago. ES&S still sells and services Premier equipment along with its own system, but Dominion owns the intellectual property rights of Premier equipment as a result of its purchase of the company.

As of this writing, Secretary Kobach has not certified the Dominion Democracy Suite. CEOs will be notified if and when certification is granted.

The Democracy Suite is a paper optical scan-based system which includes precinct ballot scanners and central scanners. The accessible ADA- and HAVA-compliant device allows a voter with a visual impairment to record his/her choices using an audio ballot and keypad. The system prints an optical scan ballot that is scanned along with other ballots. ■

Sedgwick County Sued Over Ballot Records

Sedgwick County Election Commissioner Tabitha Lehman was sued by a person seeking public access to Real Time Audit Logs (RTALs) on electronic voting machines. RTAL is ES&S's trade name for a voter verifiable paper audit trail (VVPAT), which is a printable electronic record of each voter's actions on the voting machine. RTAL documents are viewable by the voter before the electronic ballot is cast. Once the voter has cast the ballot the documents are randomly stored in the system's memory.

Elizabeth Clarkson v. Sedgwick County Elections Commissioner Tabitha Lehman was filed in state district court in Sedgwick County on June 18, 2013. The plaintiff sought access to RTAL records pursuant to the Kansas Open Records Act in order to conduct a post-election audit of the results of the November 2010 election.

In response to the plaintiff's original request for records, the election office provided precinct-based results tapes but denied the request for individual ballot logs, citing K.S.A. 25-2422 and the unnecessary burden and expense required to produce the records. State law does provide limited access to election records in a recount, but the law does not have specific provisions related to VVPATs or RTALs. These arguments were detailed in a response filed in court in July.

The court ruled in favor of the election commissioner's office. ■



SOS Holiday Hours

In observance of the regular calendar of state holidays, the secretary of state's office will be closed on the following dates:

December 25, 2013, for Christmas Day, and **January 1, 2014**, for New Year's Day.

In addition, the office will be closed Monday, **January 20, 2014** in observance of Martin Luther King, Jr. Day.

Happy Holidays from the SOS office!





PRIVACY IMPACT ASSESSMENT (PIA)

For the

SAFE - SAFE ACCESS FILE EXCHANGE

Aviation and Missile Research, Development, and Engineering Center; RDECOM

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- New DoD Information System
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number. Consult the Component Privacy Office for additional information or access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office

Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The U.S. Army Aviation and Missile Research Development and Engineering Center (AMRDEC) Safe Access File Exchange system is designed for securely exchanging various types of electronic files. It was created to provide users the capability to send/receive large files. Safe Access File Exchange primary function is strictly used as a transfer mechanism for large data files. Safe Access File Exchange can be used by anyone sending files to individuals with a .mil or .gov e-mail addresses. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format. SAFE use the latest web browser transport encryption protocols.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The security risk associated with maintaining PII in an electronic environment has been identified and mitigated through administrative, technical, and physical safeguards as well as with policy and procedures for handling, using, maintaining PII and training for authorized users of PII data. Due to the stringent safeguards and access requirements, the system and data are secure and it is unlikely that the data would be compromised or provided to any unauthorized individuals or agencies.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

Within the DoD Component.

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

Other DoD Components.

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

Other Federal Agencies.

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

State and Local Agencies.

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

Contractor (Enter name and describe the language in the contract that safeguards PII.)

Specify. Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

Other (e.g., commercial providers, colleges).

Specify.

i. **Do individuals have the opportunity to object to the collection of their PII?**

Yes

No

(1) If "Yes," describe method by which individuals can object to the collection of PII.

By not Sending any PII through the SAFE transfer system.

(2) If "No," state the reason why individuals cannot object.

j. **Do individuals have the opportunity to consent to the specific uses of their PII?**

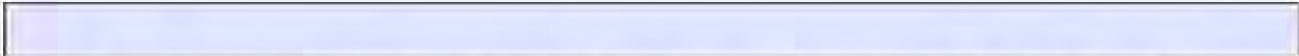
Yes

No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

By not Sending any PII through the SAFE transfer system.

(2) If "No," state the reason why individuals cannot give or withhold their consent.



k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

Privacy Act Statement

Privacy Advisory

Other

None

Describe each applicable format.

Safe Access File Exchange is approved for the transfer of For Official Use Only files in any format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

Administration of Barack Obama, 2015

Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology

March 19, 2015

Memorandum for the Secretary of Defense, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the National Security Advisor, and the Director of the Office of Administration

Subject: Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to improve the information resources and information systems provided to the President, Vice President, and Executive Office of the President (EOP), I hereby direct the following:

Section 1. Policy. The purposes of this memorandum are to ensure that the information resources and information systems provided to the President, Vice President, and EOP are efficient, secure, and resilient; establish a model for Government information technology management efforts; reduce operating costs through the elimination of duplication and overlapping services; and accomplish the goal of converging disparate information resources and information systems for the EOP.

This memorandum is intended to maintain the President's exclusive control of the information resources and information systems provided to the President, Vice President, and EOP. High-quality, efficient, interoperable, and safe information systems and information resources are required in order for the President to discharge the duties of his office with the support of those who advise and assist him, and with the additional assistance of all EOP components. The responsibilities that this memorandum vests in the Director of White House Information Technology, as described below, have been performed historically within the EOP, and it is the intent of this memorandum to continue this practice.

The Director of White House Information Technology, on behalf of the President, shall have the 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. Nothing in this memorandum may be construed to delegate the ownership, or any rights associated with ownership, of any information resources or information systems, nor of any record, to any entity outside of the EOP.

Sec. 2. Director of White House Information Technology. (a) There is hereby established the Director of White House Information Technology (Director). The Director shall be the senior officer responsible for the information resources and information systems provided to the President, Vice President, and EOP by the Presidential Information Technology Community (Community). The Director shall:

- (i) be designated by the President;
 - (ii) have the rank and status of a commissioned officer in the White House Office;
- and

(iii) have sufficient seniority, education, training, and expertise to provide the necessary advice, coordination, and guidance to the Community.

(b) The Deputy Chief of Staff for Operations shall provide the Director with necessary direction and supervision.

(c) The Director shall ensure the effective use of information resources and information systems provided to the President, Vice President, and EOP in order to improve mission performance, and shall have the appropriate authority to promulgate all necessary procedures and rules governing these resources and systems. The Director shall provide policy coordination and guidance for, and periodically review, 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 evaluation processes.

(d) The Director may advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties under this memorandum.

Sec. 3. Executive Committee for Presidential Information Technology. There is hereby established an Executive Committee for Presidential Information Technology (Committee). The Committee consists of the following officials or their designees: 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.

Sec. 4. Administration. (a) The President or the Deputy Chief of Staff for Operations may assign the Director and the Committee any additional functions necessary to advance the mission set forth in this memorandum.

(b) The Committee shall advise and make policy recommendations to the Deputy Chief of Staff for Operations and the Director with respect to operational and procurement decisions necessary to achieve secure, seamless, reliable, and integrated information resources and information systems for the President, Vice President, and EOP. The Director shall update the Committee on both strategy and execution, as requested, including collaboration efforts with the Federal Chief Information Officer, with other government agencies, and by participating in the Chief Information Officers Council.

(c) The Secretary of Defense shall designate or appoint a White House Technology Liaison for the White House Communications Agency and the Secretary of Homeland Security shall designate or appoint a White House Technology Liaison for the United States Secret Service. Any entity that becomes a part of the Community after the issuance of this memorandum shall designate or appoint a White House Technology Liaison for that entity. The designation or appointment of a White House Technology Liaison is subject to the review of, and shall be made in consultation with, the President or his designee. The Chief Information Officer of the Office of Administration and the Chief Information Officer of the National Security Council, and their successors in function, are designated as White House Technology Liaisons for their respective components. In coordination with the Director, the White House Technology Liaisons shall ensure that the day-to-day operation of and long-term

strategy for information resources and information systems provided to the President, Vice President, and EOP are interoperable and effectively function as a single, modern, and high-quality enterprise that reduces duplication, inefficiency, and waste.

(d) The President or his designee shall retain the authority to specify the application of operating policies and procedures, including security measures, which are used in the construction, operation, and maintenance of any information resources or information system provided to the President, Vice President, and EOP.

(e) Presidential Information Technology Community entities shall:

(i) assist and provide information to the Deputy Chief of Staff for Operations and the Director, consistent with applicable law, as may be necessary to implement this memorandum; and

(ii) as soon as practicable after the issuance of this memorandum, enter into any memoranda of understanding as necessary to give effect to the provisions of this memorandum.

(f) As soon as practicable after the issuance of this memorandum, EOP components shall take all necessary steps, either individually or collectively, to ensure the proper creation, storage, and transmission of EOP information on any information systems and information resources provided to the President, Vice President, and EOP.

Sec. 5. Definitions. As used in this memorandum:

(a) "Information resources," "information systems," and "information technology" have the meanings assigned by section 3502 of title 44, United States Code.

(b) "Presidential Information Technology Community" means the entities that provide information resources and information systems to the President, Vice President, and EOP, including:

- (i) the National Security Council;
- (ii) the Office of Administration;
- (iii) the United States Secret Service;
- (iv) the White House Military Office; and
- (v) the White House Communications Agency.

(c) "Executive Office of the President" means:

- (i) each component of the EOP as is or may hereafter be established;
- (ii) any successor in function to an EOP component that has been abolished and of which the function is retained in the EOP; and
- (iii) the President's Commission on White House Fellowships, the President's Intelligence Advisory Board, the Residence of the Vice President, and such other entities as the President from time to time may determine.

Sec. 6. General Provisions. (a) Nothing in this memorandum shall be construed to impair or otherwise affect:

- (i) the authority granted by law to an executive department, agency, entity, office, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(c) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

Categories: Communications to Federal Agencies : White House Information Technology, Director, memorandum establishing; Executive Committee for Presidential Information Technology, memorandum establishing.

Subjects: White House Office : Assistants to the President :: White House Information Technology, Director; White House Office : Information Technology, Executive Committee for Presidential.

DCPD Number: DCPD201500185.

the WHITE HOUSE



From the Press Office

[Speeches & Remarks](#)

[Press Briefings](#)

[Statements & Releases](#)

[Nominations & Appointments](#)

[Presidential Actions](#)

[Legislation](#)

[Disclosures](#)

The White House

Office of the Vice President

For Immediate Release

June 28, 2017

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

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

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

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

JA000219

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

[HOME](#)[BRIEFING ROOM](#)[ISSUES](#)[THE ADMINISTRATION](#)[PARTICIPATE](#)[1600 PENN](#)[USA.gov](#)[Privacy Policy](#)[Copyright Policy](#)



Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable Elaine Marshall
Secretary of State
PO Box 29622
Raleigh, NC 27626-0622

Dear Secretary Marshall,

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

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

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

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

JA000221

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

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

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

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

Sincerely,

A handwritten signature in black ink that reads "Kris Kobach". The signature is written in a cursive, slightly slanted style.

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

Privacy error x

← → ↻ **Not Secure** <https://safe.amrdec.army.mil/safe/Welcome.aspx> ☆



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). NET::ERR_CERT_AUTHORITY_INVALID

Automatically send some system information and page content to Google to help detect dangerous apps and sites. [Privacy policy](#)

Washington DC, USA - current and ac...

Secure <https://www.timeanddate.com/world>

timeanddate.com

Local time in Washington DC
Monday, July 3, 2017

12:02:40 am

EDT

Back to safety

July 3, 2017

National Association of State Secretaries
444 North Capitol Street NW, Suite 401
Washington, DC 20001

Dear State Secretaries:

We write to you regarding the recent letter from the Presidential Advisory Commission on Election Integrity (“PACEI”) to state election officials, requesting detailed personal information from your state voter registration records.¹ We are technical experts, legal scholars, and representatives of organizations expert in election integrity, voting verification, and voter privacy. We strongly oppose the PACEI request for voter record information and urge you not to comply.

The PACEI is seeking:

“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.”

This is sensitive, personal information that individuals are often required to provide to be eligible to vote. There is no indication how the information will be used, who will have access to it, or what safeguards will be established.² Moreover, it appears that the Presidential Commission has failed to undertake and publish a Privacy Impact Assessment, required by federal law, prior to the collection of personal data.³

Although the standards vary across the country, there is no question that voter privacy -- and the secret ballot in particular -- are integral to the American system of democracy. It is absolutely unprecedented for the federal government to demand the production of voter records from the states.

As custodians of voter data, you have a specific responsibility to safeguard voter record information. We urge you to protect the rights of the voters in your states and to oppose the request from the PACEI.

¹ See, e.g., Letter from Kris W. Kobach, Vice Chair, PACEI, to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017).

² See EPIC, “Voter Privacy and the PACEI,” epic.org/privacy/voter/pacei/.

³ Pub.Law 107-347, 44 U.S.C. § 3501 (Note). See also “M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002” (Sept. 26, 2003).

For further information regarding this statement, please contact EPIC President Marc Rotenberg (rotenberg@epic.org) or EPIC Policy Director Caitriona Fitzgerald (fitzgerald@epic.org).

ORGANIZATIONS

Electronic Privacy Information Center (EPIC)
American Library Association
Center for Democracy & Technology
Center for Media and Democracy
Center for Media Justice
Constitutional Alliance
Consumer Federation of America
Consumer Action
Consumer Watchdog
Cyber Privacy Project
Defending Rights & Dissent
Federation of American Scientists
Government Accountability Project
Lawyers for Good Government
Liberty Coalition
National Center for Transgender Equality
National Network to End Domestic Violence
New America's Open Technology Institute
Patient Privacy Rights
Privacy Rights Clearinghouse
Privacy Times
RootsAction.org
World Privacy Forum

INDIVIDUAL EXPERTS

Alessandro Acquisti, Professor, Carnegie Mellon University
Ann Bartow, Professor of Law, University of New Hampshire School of Law
Francesca Bignami, Professor of Law, The George Washington University Law School
Christine L. Borgman, Distinguished Professor & Presidential Chair in Information Studies, UCLA
Kimberly Bryant, Founder/Executive Director, Black Girls CODE
David Chaum, Voting Systems Institute
Danielle Keats Citron, Morton & Sophia Macht Professor of Law, University of Maryland Carey School of Law
Julie E. Cohen, Mark Cluster Mamolen Professor of Law and Technology, Georgetown Law
Jennifer Daskal, Associate Professor, American University Washington College of Law
Cynthia Dwork, Distinguished Scientist, Microsoft Research

Voter Privacy Experts and Organizations 2
Opposition to Demand for State Records

Letter to State Secretaries
July 3, 2017

David J. Farber, Distinguished Career Professor of Computer Science and Public Policy,
Carnegie Mellon University
Michael Fischer, Professor of Computer Science, Yale University
Martin Hellman, Member, US National Academy Engineering, Professor Emeritus of
Electrical Engineering, Stanford University
Candice Hoke, Co-Director, Center for Cybersecurity & Privacy Protection, Professor of
Law, C|M Law, Cleveland State University
Deborah Hurley, Harvard University and Brown University
Dr. David Jefferson, Visiting Scientist, Lawrence Livermore National Laboratory
Jeff Jonas, Founder and Chief Scientist, Senzing
Douglas W. Jones, Department of Computer Science, University of Iowa, coauthor of
Broken Ballots: Will Your Vote Count, CSLI, 2012
Lou Katz, Ph.D., founder, Usenix Association
Pamela S. Karlan, Kenneth and Hale Montgomery Professor of Public Interest Law, Co-
Director, Supreme Court Litigation Clinic, Stanford Law School
Joe Kiniry, CEO and Chief Scientist, Free & Fair
Chris Larsen, Executive Chairman, Ripple, Inc.
Harry Lewis, Gordon McKay Professor of Computer Science, Harvard University
Anna Lysyanskaya, Professor of Computer Science, Brown University
Gary T. Marx, Professor Emeritus of Sociology, MIT
Mary Minow, Senior Fellow, Advanced Leadership Initiative, Harvard University
Dr. Pablo Molina, Adjunct Professor, Georgetown University
Jennifer L. Mnookin, Dean and David G. Price & Dallas P. Price Professor of Law, UCLA
School of Law
Eben Moglen, Professor of Law, Columbia Law School
Erin Murphy, Professor of Law, NYU School of Law
Peter G. Neumann, Computer Science Laboratory, SRI International
Helen Nissenbaum, Professor, NYU + Cornell Tech
Frank Pasquale, Professor of Law, University of Maryland Carey School of Law
Ron Rivest, MIT Institute Professor
Pam Samuelson, Richard M. Sherman Distinguished Professor of Law, Berkeley Law
School
Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School
Barbara Simons, Ph.D., IBM Research (retired)
Robert Ellis Smith, publisher, *Privacy Journal*
Eugene H. Spafford, Professor, Purdue University
Philip B. Stark, Associate Dean, Mathematical and Physical Sciences, Professor,
Department of Statistics, University of California
Nadine Strossen, John Marshall Harlan II Professor of Law, New York Law School;
Former President, American Civil Liberties Union
Frank Turkheimer, Professor of Law Emeritus, University of Wisconsin Law School
Sherry Turkle, Abby Rockefeller Mauzé Professor of the Social Studies of Science and
Technology, Massachusetts Institute of Technology
Poorvi L. Vora, Professor of Computer Science, The George Washington University

Jim Waldo, Gordon McKay Professor of the Practice, Chief Technology Officer, Harvard University

Anne L. Washington, Assistant Professor, Schar School of Policy and Government, George Mason University

Chris Wolf, Board Chair, Future of Privacy Forum

Shoshana Zuboff, Charles Edward Wilson Professor of Business Administration, Retired

(affiliations are for identification only)



The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

2 Martin Luther King Jr., Drive
802 West Tower
Atlanta, Georgia 30334

Chris Harvey
DIRECTOR OF ELECTIONS

July 3, 2017

VIA EMAIL

The Honorable Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

RE: Open Records Request Dated June 28, 2017

Dear Secretary Kobach,

This letter is in response to your request dated June 28, 2017 in which you seek the publicly-available voter roll data for Georgia. Under Georgia law (O.C.G.A. § 21-2-225), information on file regarding Georgia's list of electors is required to be available to the public upon request, except that the day and month of birth, social security number, driver's license number, and the locations at which electors applied to vote are confidential and not subject to disclosure.

Two years ago, our office reformed its process of handling public record requests to be more secure. In order to provide the publicly available information, our security protocol requires certain steps to be followed. Upon receipt, our office will prepare the publicly-available list of electors data file. The data file will undergo a thorough review process to ensure confidential information is not included before it is sent by secure means to the Commission. The data file will be encrypted and password protected.

Also, in order to process and send the requested publicly-available records, our office requires pre-payment of the \$250 statewide file fee. Please send check or money order payable to the "Georgia Secretary of State" to my attention at the address in the header of this letter.

Sincerely,

Chris Harvey
Director of Elections
Georgia Secretary of State's Office

JA000228

DECLARATION OF MARC ROTENBERG

I, Marc Rotenberg, declare as follows:

1. I am President and Executive Director for the Plaintiff Electronic Privacy Information Center (“EPIC”).
2. Plaintiff EPIC is a non-profit corporation located in Washington, D.C. EPIC is a public interest research center, which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC has a particular interest in preserving privacy safeguards established by Congress, including the E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note), EPIC pursues a wide range of activities designed to protect privacy and educate the public, including policy research, public speaking, conferences, media appearances, publications, litigation, and comments for administrative and legislative bodies regarding the protection of privacy.
3. I am a member in good standing of the Bar of the District of Columbia (admitted 1990), the Bar of Massachusetts (1987), the U.S. Supreme Court (1991), the U.S. Court of Appeals—1st Circuit (2005), the U.S. Court of Appeals—2nd Circuit (2010), the U.S. Court of Appeals—3rd Circuit (1991) the U.S. Court of Appeals—4th Circuit (1992), the U.S. Court of Appeals—5th Circuit (2005), the U.S. Court of Appeals—7th Circuit (2011), the U.S. Court of Appeals—9th Circuit (2011), and the U.S. Court of Appeals—D.C. Circuit (1991).
4. I have taught Information Privacy Law continuously at Georgetown University Law Center since 1990.
5. I am co-author with Anita Allen of a leading casebook on privacy law.

6. In my capacity as President and Executive Director, I have supervised both EPIC's response to the Department's rulemaking and EPIC'S participation in all stages of litigation in the above-captioned matter.
7. The statements contained in this declaration are based on my own personal knowledge.
8. EPIC works with an Advisory Board consisting of nearly 100 experts from across the United States drawn from the information law, computer science, civil liberties and privacy communities.
9. Members of the EPIC Advisory Board must formally commit to joining the organization and to supporting the mission of the organization.
10. Members of the EPIC Advisory Board make financial contributions to support the work of the organization.
11. Members of the EPIC Advisory Board routinely assist with EPIC's substantive work. For example, members provide advice on EPIC's projects, speak at EPIC conferences, and sign on to EPIC amicus briefs.
12. In this matter, EPIC represented the interests of more than 30 members of the EPIC Advisory Board, who signed a Statement to the National Association of State Secretaries in Opposition to the Commission's demand for personal voter data.

Under penalty of perjury, I declare that the foregoing is true and correct to the best of my knowledge and belief.



Marc Rotenberg
EPIC President and Executive Director

Executed this 7th day of July, 2017



Privacy Impact Assessments (PIA)

GSA collects, maintains and uses personal information on individuals to carry out the agency's mission and responsibilities and to provide services to the public. By federal law and regulation, privacy issues and protections must be considered for information technology systems that contain any personally identifiable information. GSA uses the Privacy Impact Assessment (PIA) as a key tool in fulfilling these legal and regulatory obligations. By conducting PIAs, GSA ensures that:

- The information collected is used only for the intended purpose;
- The information is timely and accurate;
- The information is protected according to applicable laws and regulations while in GSA's possession;
- The impact of the information systems on individual privacy is fully addressed; and
- The public is aware of the information GSA collects and how the information is used.

PIA Systems

System Title	Acronym/Short Name
ACMIS	ACMIS [PDF - 222 KB]
Challenge.gov	Challenge.gov [DOC - 206 KB]
Childcare Subsidy	CCS [PDF - 329 KB]
Citizen Engagement Platform	CEP [DOC - 100 KB]
ClearPath Hosting Services	GSA FSS-13 [PDF - 189 KB]
Controlled Document Tracker	CDT [PDF - 107 KB]
Customer Engagement Organization	CEO [DOC - 120 KB]
Data.gov	Data.gov [PDF - 300 KB]
Data Leakage Prevention	DLP [PDF - 173 KB]
Digital.gov	Digital.gov [PDF - 474 KB]
eGOV Jobcenter	eGOV Jobcenter [PDF - 199 KB]
eLease	eLease [PDF - 144 KB]
Electronic Acquisition System - Comprizon	EAS-Comprizon [PDF - 158 KB]
Electronic Document Management Software	EDMS [PDF - 49 KB]
EMD	EMD [PDF - 202 KB]
E-PACS	E-PACS [PDF - 48 KB]
E-Travel Carlson Wagonlit Government Travel E2 Solutions	E2Solutions [PDF - 174 KB]
E-Travel Northrop Grumman Mission Solutions - GovTrip	E-Travel GovTrip [PDF - 227 KB]
FAI On-Line University	FAI [PDF - 113 KB]
FAR Data Collection Pilot	FAR [PDF - 51 KB]
FBO	FBO [PDF - 489 KB]
Federal Personal Identity Verification Identity Management System	PIV IDMS [PDF - 222 KB]
ImageNow	ImageNow [PDF - 145 KB]
JP Morgan Chase	JP Morgan [PDF - 55 KB]
Login.gov	Login.gov [PDF - 196 KB]
National Contact Center (NCC)	NCC [PDF - 172 KB]
Office of Inspector General Information System	OIGMIS [PDF - 161 KB]
Office of Inspector General Counsel Files	GSA/ADM-26 [DOC - 38 KB]

System Title	Acronym/Short Name
OGC Case Tracking	OGC [PDF - 3 KB]
Open Government Citizen Engagement Tool	OGC Engagement [PDF - 384 KB]
ORC	ORC [PDF - 211 KB]
Payroll Accounting and Reporting (PAR)	PAR [PDF - 245 KB]
Pegasys	Pegasys [PDF - 54 KB]
PPFM 8 Chris	PPFM 8 [PDF - 65 KB]
Sales Automation System	SASy [DOC - 104 KB]
Social Media Platforms	Social Media [PDF - 84 KB]
STAR	STAR [DOC - 259 KB]
System for Award Management (SAM)	SAM [DOC - 39 KB]
The Museum System	TMS [PDF - 141 KB]
Transit	Transit [PDF - 195 KB]
USA.gov	USA.gov [PDF - 424 KB]
USAccess	USAccess [PDF - 240 KB]

CONTACTS

GSA Privacy Act Officer

- [View Contact Details](#)

PIA POLICY

- [1878.2A CIO P - Conducting Privacy Impact Assessments \(PIAs\) in GSA](#)

PIA TEMPLATES

- [PIA Template](#)
- [PIA template for Agency Use of Third-Party Websites and Applications](#)

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.

Civil Action No. 1:17-cv-1320 (CKK)

DECLARATION OF CHARLES CHRISTOPHER HERNDON

I, Charles C. Herndon, declare as follows:

1. I am the Director of White House Information Technology (“WHIT”) and Deputy Assistant to the President. I am the senior officer responsible for the information resources and information systems provided to the President, Vice President and Executive Office of the President. I report to White House Deputy Chief of Staff for Operations and Assistant to the President, and through him to the Chief of Staff and the President. I am part of what is known as the White House Office. This declaration is based on my personal knowledge and upon information provided to me in my official capacity.

2. A number of components make up the Executive Office of the President, including the White House Office (also referred to as the Office of the President). Components of the White House Office include the President’s immediate staff, the White House Counsel’s Office and the Staff Secretary’s Office. The White House Office serves the President in the performance of the many detailed activities incident to his immediate office, and the various

Assistants and Deputy Assistants to the President aid the President in such matters as he may direct. My role is to ensure the effective use of information resources and systems to the President. I am also a member of the Executive Committee for Presidential Information Technology, as established in the March 19, 2015, Presidential Memorandum creating my position. See, <https://obamawhitehouse.archives.gov/the-press-office/2015/03/19/presidential-memorandum-establishing-director-white-house-information-te>. [The Executive Committee is chaired by the Deputy Chief of Staff Operations.](#)

3. I was asked by the Office of the Vice President to assist in creating a mechanism by which data could be securely loaded and stored within the White House computer systems. To do that I repurposed an existing system that regularly accepts personally identifiable information through a secure, encrypted computer application within the White House Information Technology system.

4. States that wish to provide information to the Presidential Advisory Commission on Election Integrity (“Commission”) can email the Commission to request an access link. Once a staff member verifies the identity of the requester and the email address, a one-time unique uniform resource locator (“URL”) link will be emailed to that state representative. Data can be uploaded via that one-time link to a server within the domain electionintegrity.whitehouse.gov. Authorized members of the Commission will be given access to the file directory identified to house the uploaded information. Once the files have been uploaded, there is no further transfer of the data from that location. The technology is similar to a shared folder in Microsoft SharePoint.

5. The Commission will receive dedicated laptops, which can access the data provided by states through the White House network over an SSL (Secure Sockets Layer)

connection. The SSL connection ensures that all data passed between the web server and browsers remain private and secure. The laptops use Personal Identity Verification (PIV) and the data at rest is encrypted.

6. The Executive Committee for Information Technology will have no role in this data collection process. The U.S. Digital Service (which is within the Office of Management and Budget) will also have no role, nor will any federal agency. The only people who will assist are a limited number of my technical staff from the White House Office of Administration. They will have access to the data, but all access will be logged and recorded by our network monitoring tools.

7. I can confirm, based on information provided to me from the Department of Defense, that the data the state of Arkansas uploaded to the Army's SAFE site has been deleted without ever having been accessed by the Commission.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 16th day of July 2017.



Digitally signed by CHARLES HERNDON
DN: c=US, o=U.S. Government, ou=Executive Office
of the President, cn=CHARLES HERNDON,
0.9.2342.19200300.100.1.1=11001003426249
Date: 2017.07.17 06:36:16 -04'00'

Charles C. Herndon

**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)

DECLARATION BY ELENI KYRIAKIDES

I, Eleni Kyriakides, declare as follows:

1. My name is Eleni Kyriakides.
2. I am an EPIC Law Fellow at the Electronic Privacy Information Center.
3. In my capacity as a Fellow, I coordinate EPIC's Open Government Project. This includes overseeing EPIC's work using the Freedom of Information Act (FOIA).
4. EPIC makes frequent use of the FOIA to obtain records on government programs implicating privacy and civil liberties. EPIC seeks public disclosure of this information to help ensure that the public is fully informed about the activities of government, and to conduct oversight and analysis of these programs.

5. By refusing to release a Privacy Impact Assessment as required by law, the Defendants have increased the burden on EPIC to conduct its “oversight and analysis” in a more costly and resource-intensive way that would not otherwise be necessary.

6. As a result, I have researched, drafted, and submitted five requests seeking details related to the Commission’s recent activities: one to the U.S. Department of Justice, two to the Commission, one to the General Services Administration, and one to the Arkansas Secretary of State Mark Martin. *See* EPIC Exhibit FOIA Requests.

I declare under penalty of perjury that, to the best of my knowledge, the forgoing is true and correct.

Executed July 17, 2017.

Respectfully Submitted,

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

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 17, 2017



Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
<https://epic.org>

VIA E-MAIL

June 30, 2017

Nelson D. Hermilla, Chief
FOIA/PA Branch
Civil Rights Division
Department of Justice
BICN Bldg., Room 3234
950 Pennsylvania Avenue, NW
Washington, DC 20530
CRT.FOIArequests@usdoj.gov

Dear Mr. Hermilla,

This letter constitutes a request under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center (“EPIC”) to the Department of Justice (“DOJ”).

On June 28, 2017, the DOJ wrote to all states covered by the National Voter Registration Act (“NVRA”) with a sweeping request for information regarding state voter registration list maintenance including “All statutes, regulations, written guidance, internal policies, or database user manuals that set out the procedures” the states have in place related to voter registration requirements, any other relevant procedures, and an explanation of the officials responsible for maintaining voter registration lists. The DOJ also sought, for local election officials, descriptions of the steps taken to ensure list maintenance is in “full compliance with the NVRA.”¹ The DOJ gave the states 30 days to comply with the request. The DOJ offered no explanation or justification for the unprecedented time-bound request, stating only that the agency “reviewing voter registration list maintenance procedures in each state covered by the NVRA.”²

Also on June 28, 2017, the Kris Kobach, the Vice Chair of the Presidential Advisory Commission on Election Integrity (“PACIE”), sent a letter to the Secretaries of State for all 50 states and the District of Columbia asking that the states provide the Commission detailed voter information, including

the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony

¹ See, e.g., Letter from T. Christian Herren, Jr., Chief, Voting Section, U.S. Dep’tment of Justice, to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections (June 28, 2017), <https://www.documentcloud.org/documents/3881855-Correspondence-DOJ-Letter-06282017.html>.

² *Id.*

convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.³

EPIC seeks two categories of records concerning the DOJ's June 28th request for information on state voter list procedures.

Records Requested

(1) All records, including memoranda, legal analyses, and communications, concerning the DOJ's June 28, 2017 request to the states regarding voter list maintenance; and

(2) All communications between the DOJ and the Presidential Advisory Commission on Election Integrity ("PACEI") regarding the June 28, 2017 PACEI request for state voter data as well as any legal memoranda concerning the authorities of the PACEI.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. 5 U.S.C. § 552(a)(6)(E)(v)(II). To warrant expedited processing, under DOJ FOIA regulations a FOIA request must concern a matter of (1) "urgency to inform the public about an actual or alleged federal government activity," and, (2) the request must be "made by a person who is primarily engaged in disseminating information." 28 C.F.R. § 16.5(e)(1)(ii). This request satisfies both requirements.

First, there is an "urgency to inform the public about an actual or alleged federal government activity." § 16.5(e)(1)(ii). The "actual... federal government activity" at issue is DOJ's request to the states covered by the National Voter Registration Act ("NVRA") for information concerning each state's "voter registration list maintenance procedures." The DOJ concedes this activity in letters to the states.⁴

"Urgency" to inform the public about this activity is clear given the extraordinary nature and unusual breadth of the DOJ's request. On June 28, 2017, DOJ requested that all states covered by the NVRA provide to the DOJ *within 30 days* a sweeping list of information about state voting list maintenance. Indeed, former DOJ civil rights official and professor Justin Levitt told *ProPublica* that "he did not recall a time when the DOJ has previously requested such broad information."⁵ Former senior litigator with the DOJ's Voting Section, David Becker called the move "unprecedented":

³ See, e.g. Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), <https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html>; See generally EPIC, *Voter Privacy and the PACEI*, <https://epic.org/privacy/voting/pacei/>.

⁴ *Id.*

⁵ Jessica Huseman, *Presidential Commission Demands Massive Amounts of State Voter Data*, *ProPublica* (June 29, 2107), <https://www.propublica.org/article/presidential-commission-demands-massive-amounts-of-state-voter-data>.

In the quarter-century since passage of the NVRA, of which I spent seven years as a DOJ lawyer enforcing the NVRA, among other laws, *I do not know of the DOJ conducting any other broad-based fishing expedition into list maintenance compliance, whether during Democratic or Republican administrations.*⁶

Former deputy assistant general for civil rights Sam Bagnestos warned: “Let’s be clear about what this letter signals: DOJ Civil Rights is preparing to sue states to force them to trim their voting rolls.”⁷

The DOJ’s request also represents a selective review of state voting processes,⁸ without any basis offered for its narrow focus. The NVRA was passed not only to ensure “accurate and current voter registration rolls,” but also “to establish procedures that will increase the number of eligible citizens who register to vote in elections for Federal office” and recognized that “the right of citizens of the United States to vote is a fundamental right.” 52 U.S.C. § 20501. For instance, the DOJ request did not include an information request for compliance NVRA requirements voter registration forms be made easily available for distribution (§ 20505(b)), for simultaneous voter registration while applying for a driver’s license (§ 20505(a)), and that state offices that provide public assistance and services to those with disabilities provide voter registration application forms and assistance (§ 20505(a)(4)(A)).

Despite the extraordinary nature of the request the DOJ offered no explanation or justification for the sudden broad-based request. The DOJ merely cited an agency review of “voter registration list maintenance procedures” in these states,⁹ and “did not respond to requests for comment about the letters.”¹⁰

States have thirty days to respond to the DOJ request. There is an urgent public need for immediate release of information explaining the DOJ’s unprecedented decision to demand this voting list information from states. Moreover, the coincidental request by the PACEI for similar information from the states raises substantial concerns that the DOJ request was part of a coordinated undertaking. The PACEI has given the states approximately two weeks to respond their request.

Second, EPIC is an organization “primarily engaged in disseminating information.” § 16.5(e)(1)(ii). As the Court explained in *EPIC v. Dep’t of Def.*, “EPIC satisfies the definition of

⁶ David Becker, *Why Wednesday’s ‘Election Integrity’ Actions Should Be Watched By States*, Route Fifty (June 29, 2017), <http://www.routefifty.com/management/2017/06/trump-election-integrity-commission-state-voter-data/139107/> (emphasis added).

⁷ @sbagen, Twitter (June 29, 2017, 1:46 PM), <https://twitter.com/sbagen/status/880528035392491520>.

⁸ *Jessica Huseman*, *supra* note 6.

⁹ See Letter from T. Christian Herren, Jr. to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections, *supra* note 1.

¹⁰ *Id.*

‘representative of the news media’” entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for “News Media” Fee Status and Fee Waiver

EPIC is a “representative of the news media” for fee classification purposes. *EPIC v. Dep’t of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC’s status as a “news media” requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information “is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest” of EPIC. 28 C.F.R. § 16.10(k)(1); § 552(a)(4)(A)(iii). EPIC’s request satisfies the FBI’s three factors for granting a fee waiver. § 16.10(k)(2).

Under the DOJ FOIA regulations, DOJ components evaluate three considerations to determine whether fee waiver is warranted: (i) the “subject of the request must concern identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated”; (ii) disclosure must be “likely to contribute significantly to public understanding of those operations or activities”; and (iii) “disclosure must not be primarily in the commercial interest of the requester.” §§ 16.10(k)(2)(i)–(iii).

First, disclosure of the requested DOJ records concerning the June 28th request to states for “voter registration list maintenance” self-evidently “concerns identifiable operations or activities of the Federal Government with a connection that is direct and clear, not remote or attenuated.” § 16.10(k)(2)(i). This request concerns a direct request from the DOJ to states for information, concerning a law that the DOJ is authorized to enforce.

Second, disclosure “would be likely to contribute significantly to public understanding of those operations or activities” according to the two sub-factors. § 16.10(k)(2)(ii)(A-B). As to the first sub-factor, disclosure would be “meaningfully informative about government operations or activities” because the justification and decision-making underlying for the DOJ’s unprecedented request to states covered by the NVRA has not been made public. § 16.10(k)(2)(ii)(A). Any additional information about how why the DOJ is seeking broad based data under only select provisions of NVRA would thus be “meaningfully informative” about the DOJ request. As to the second sub-factor, disclosure will “contribute to the understanding of a reasonably broad audience of persons interested in the subject,” because, as stated in the relevant FOIA regulations, components will “presume that a representative of the news media will satisfy this consideration.” § 16.10(k)(2)(ii)(B).

Third, disclosure of the requested information is not “primarily in the commercial interest” of EPIC according to the two sub-factors. § 16.10(k)(2)(iii)(A-B). As to the first sub-factor, EPIC

has no “commercial interest...that would be furthered by the requested disclosure.” § 16.10(k)(2)(iii)(A). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.¹¹ As to the second sub-factor, “the component must determine whether that is the primary interest furthered by the request” because, as stated in the FOIA regulations, DOJ “ordinarily will presume that where a news media requester has satisfied [the public interest standard], the request is not primarily in the commercial interest of the requester.” § 16.10(k)(2)(iii)(B). As already described above, EPIC is a news media requester and satisfies the public interest standard.

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within ten calendar days 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

¹¹ *About EPIC*, EPIC.org, <http://epic.org/epic/about.html>.

VIA E-Mail

July 4, 2017

Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

Dear Sir or Madam:

This letter constitutes a request under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center (“EPIC”) to the Presidential Commission on Election Integrity (“PACEI” or “Commission”).

This is a request for records in possession of the agency concerning the letters that were sent on or about June 28, 2017 requesting the production of state voter records and other related information.

Background

The Presidential Advisory Commission on Election Integrity was established by executive order on May 11, 2017.¹ On June 28, 2017, the Commission undertook an effort to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

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.²

The Vice Chair indicated that the Commission expected a response from the states by July 14, 2017.³

Such a request to state election officials had never been made by any federal official before. Election officials across the political spectrum in at least two dozen states have already partially or fully refused to comply with PACEI’s request.⁴

¹ Exec. Order No. 13,799, 82 Fed. Reg. 22, 389 (May 11, 2017).

² Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Sec’y of State, North Carolina (June 28, 2017), <https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html>.

³ *Id.*

⁴ Philip Bump & Christopher Ingraham, *Trump Says States Are ‘Trying to Hide’ Things from His Voter Fraud Commission. Here’s What They Actually Say*, Wash. Post (July 1, 2017),

On June 28th, the U.S. Department of Justice issued a parallel request. The DOJ wrote to all states covered by the National Voter Registration Act with a similarly unprecedented demand for information regarding compliance with state voter registration list maintenance.⁵ The DOJ gave the states 30 days to comply with the request.

EPIC seeks nine categories of records from the agency concerning the Commission's June 28th, 2017 request to state election officials.

Records Requested

- (1) All communications to state election officials regarding the request;
- (2) All communications between and amongst Commission staff and Commission members regarding the request;
- (3) All communications between the Commission staff and the Department of Justice and all communications between Commission members and the Department of Justice regarding the request;
- (4) All records concerning compliance with the E-Government Act of 2002 and the specific obligation to undertake a Privacy Impact Assessment;
- (5) All records concerning compliance with the Federal Advisory Committee Act and the failure to post a Privacy Impact Assessment;
- (6) All records concerning compliance with the Privacy Act of 1974 and the failure to undertake a Systems of Records Notice;
- (7) All records concerning the decision to use an insecure website and an insecure email address to receive state voter data;
- (8) All legal memorandum concerning the Commission's authority to request personal data from the states; and
- (9) Such other records that assess the privacy and security risks of aggregating nearly two hundred million voter records in a federal database.

https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.

⁵ See, e.g., Letter from T. Christian Herren, Jr., Chief, Voting Section, U.S. Dep'tment of Justice, to Kim Westbrook Strach, Exec. Dir., North Carolina State Bd. Of Elections (June 28, 2017), <https://www.documentcloud.org/documents/3881855-Correspondence-DOJ-Letter-06282017.html>.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. To warrant expedited processing, a FOIA request must concern a “compelling need.” 5 U.S.C. § 552(a)(6)(E)(i). “Compelling need” is demonstrated where the request is (1) “made by a person primarily engaged in disseminating information,” with (2) “urgency to inform the public concerning actual or alleged Federal Government activity.” § 552(a)(6)(E)(v)(II). This request satisfies both requirements.

First, EPIC is an organization “primarily engaged in disseminating information.” § 552(a)(6)(E)(v)(II). As the Court explained in *EPIC v. DOD*, “EPIC satisfies the definition of ‘representative of the news media.’” 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Second, there is an “urgency to inform the public about an actual or alleged Federal Government activity.” § 552(a)(6)(E)(v)(II). The “actual...Federal Government activity” at issue is PACEI’s request to states for detailed voter history information. The PACEI concedes this activity in letters to the states.⁶

“Urgency” to inform the public about this activity is clear given the extraordinary nature of PACEI’s sweeping request for voter data.⁷ On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* – disclose sensitive, personal information that individuals are often required to provide to be eligible to vote. To date, PACEI has not indicated how the information will be used, who will have access to it, or what safeguards will be established. PACEI has also not made any Privacy Impact Assessment for the collection of state voter data.

As noted already, state officials in over two dozen states have partially or fully opposed PACEI’s demand.⁸ Mississippi Secretary of State Delbert Hosemann stated, “They can go jump in the Gulf of Mexico.”⁹ California Secretary of State Alex Padilla added that he would “not provide sensitive voter information to a committee that has already inaccurately passed judgment that millions of Californians voted illegally. California’s participation would only serve to legitimize the false and already debunked claims of massive voter fraud.”¹⁰ Kentucky’s Secretary of State

⁶ See Letter from Kris Kobach to Elaine Marshall, *supra* note 2.

⁷ *Voter Privacy and the PACEI*, Epic.org, <https://epic.org/privacy/voting/pacei/>.

⁸ See Philip Bump & Christopher Ingraham, *supra* note 4.

⁹ Editorial Board, *Happy Fourth of July! Show Us Your Papers*, N.Y. Times (July 3, 2017), <https://mobile.nytimes.com/2017/07/03/opinion/voter-fraud-data-kris-kobach.html>.

¹⁰ Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017), <http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/>.

Alison Lundergan Grimes concluded, “There's not enough bourbon here in Kentucky to make this request seem sensible.”¹¹

Fifty technical experts and legal scholars and twenty organizations expert in election integrity, voting verification, and voter privacy also recorded opposition to PACEI’s request. In a letter to state officials, they explained: “As custodians of voter data, you have a specific responsibility to safeguard voter record information.”¹²

This request concerns a matter of widespread public concern; the right to vote is protected by the U.S. Constitution. U.S. Const. amends. XV, XIX, XXIV, XXVI. Voter privacy and the secret ballot are unquestionably integral to American democracy.

States have only days left to respond to PACEI’s request. There is an urgent public need for immediate release of information explaining the PACEI’s unprecedented decision to collect, en masse, voters’ personal information from the states. Moreover, the coincidental request by the DOJ for similar information from the states raises substantial concerns that the PACEI request was part of a coordinated undertaking.¹³

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for “News Media” Fee Status and Fee Waiver

EPIC is a “representative of the news media” for fee classification purposes. *EPIC v. Dep’t of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC’s status as a “news media” requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information “is in the public interest” because (1) “it is likely to contribute significantly to public understanding of the operations or activities of the government,” and (2) disclosure “is not primarily in the commercial interest” of EPIC. § 552(a)(4)(A)(iii).

First, disclosure of the requested PACEI records concerning the June 28th request to states for detailed voter histories “is likely to contribute significantly to public understanding of the operations or activities of the government.” § 552(a)(4)(A)(iii). The requested PACEI records self-evidently concerns “operations or activities of the government.” *Id.* This request concerns a direct

¹¹ Max Greenwood, *Kentucky secretary of state: 'Not enough bourbon in Kentucky' to make me release voter data*, Hill (June 30, 2017), <http://thehill.com/homenews/state-watch/340331-kentucky-secretary-of-state-not-enough-bourbon-in-kentucky-to-make-me>.

¹² Letter from Organizations and Individual Experts to National Association of State Secretaries (July 3, 2017), <https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf>.

¹³ See Letter from Eleni Kyriakides, EPIC Law Fellow, to Nelson Hermilla, Chief, FOIA/PA Branch, Civil Rights Div. (June 30, 2017), <https://epic.org/privacy/voting/EPIC-17-06-30-DOJ-20170630-Request.pdf>

request from a presidential commission to state officials to obtain state voter information. Disclosure of the PACEI records is also “likely to contribute significantly to public understanding” of the Commission’s activities because, despite the extraordinary nature of PACEI’s demand, the Commission has not explained how it plans to use, protect, or dispose of the sensitive personal data requested. § 552(a)(4)(A)(iii). Any additional information about how and why PACEI is seeking this data would “contribute significantly” to the public’s understanding of PACEI’s activities.

Second, disclosure of the requested information is not “primarily in the commercial interest” of EPIC. § 552(a)(4)(A)(iii). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.¹⁴

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within ten calendar days 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.




Respectfully submitted,

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow

¹⁴ *About EPIC*, EPIC.org, <http://epic.org/epic/about.html>.



Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

 +1 202 483 1140
 +1 202 483 1248
 @EPICPrivacy
 <https://epic.org>

VIA MAIL & FOIAonline

June 12, 2017

U.S. General Services Administration
FOIA Requester Service Center (H1F)
1800 F Street, NW, Room 7308
Washington, DC 20405-0001

Dear Sir/Madam,

This letter constitutes an urgent request under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center (“EPIC”) to the General Services Administration (“GSA”).

EPIC seeks records in possession of the agency concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 letter from the Presidential Advisory Commission on Election Integrity (the “Commission”).

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

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.¹

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.² Further, the letter from the Commission indicated no familiarity with the data that may disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

¹ See, e.g. Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), <https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html>.

² Lewis Decl. Ex. 11., EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

Following a proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.³

The Arkansas Secretary of State's Office charges \$2.50 per statewide voter registration data file.⁴ A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.⁵ The Office provides three types of files, with three clearly defined sets of information:

(1) "...Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."

(2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And

(3) "...a combination of the Voter Registration and Vote History files (VRVH)."⁶

The files are provided in ".CSV format" and "are available in CD format for pickup at the State Capitol Building or by mail" or "can also be placed on an FTP site."⁷

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

(1) All records indicating payment by the Commission to obtain Arkansas voter records;

(2) The completed "Data Request Forms," prepared by the Commission to obtain the Arkansas state vote records;

(3) All records indicating the types of data transferred by Arkansas to the Commission; and

³ Transcript of Temporary Restraining Order at 40, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017).

⁴ *Voter Data Request Form*, Arkansas.gov
<http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf> (last visited July 12, 2017).

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

(4) All records indicating the Commission's compliance with the Arkansas procedures to obtain state voter records.

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request because this request involves a "compelling need." 5 U.S.C. § 552(a)(6)(E)(i). Specifically, under GSA FOIA regulations a request warrants expedited processing where the information sought is (1) "urgently needed," (2) "by an individual primarily engaged in disseminating information," and (3) "in order to inform the public concerning actual or alleged Federal Government activity." 41 C.F.R. § 105-60.402-2(c)(2). This request satisfies all three requirements.

First, records concerning the Arkansas voter data transfer to the SAFE website, obtained following the June 28th request, is "urgently needed." § 105-60.402-2(c)(2). This information "has a particular value that will be lost if not disseminated quickly." *Id.* Indeed, this request concerns *both* a "breaking news story" and an issue of significant "general public interest." *Id.* On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* - disclose sensitive, personal information individuals are often required to provide to be eligible to vote. Since that date, public interest in the PACEI's demand for state election officials to transfer personal voter data has dominated the news cycle, driven by prompt dissent of state officials in at least two dozen states across the political spectrum and public outcry.⁸ Following PACEI's request less than two weeks ago, "[t]en states noted at least a slight increase in citizen calls and emails, and some citizens inquired about the process to unregister to vote, or how to secure their personal information."⁹

On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.¹⁰ There are approximately 1.7 million registered voters in the state of Arkansas potentially implicated by this transfer.¹¹ The Commission will hold its first meeting on July 19, 2017.¹² Ahead of that meeting, the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

⁸ Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.

⁹ Dylan Wells & Saisha Talwar, *Some voters un-registering following Trump administration's data requests*, ABC News (July 11, 2017), <http://abcnews.go.com/Politics/voters-registering-trump-administrations-data-requests/story?id=48578555>.

¹⁰ Transcript of Temporary Restraining Order at 40, *supra* note 3.

¹¹ *Registered Voters [As of 6/1/16]*, Arkansas.gov <http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf> (last visited July 12, 2017).

¹² Meeting notice, 82 FR 31063 (July 5, 2017).

Second, EPIC is an organization “primarily engaged in disseminating information,” § 105-60.402-2(c)(2). As the Court explained in *EPIC v. Dep’t of Def.*, “EPIC satisfies the definition of ‘representative of the news media’” entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Third, this request involves “actual... federal government activity.” § 105-60.402-2(c)(2). This FOIA concerns PACEI’s request to states for detailed voter history information, conceded by PACEI in letters to the states,¹³ and the transfer of Arkansas voter data to PACEI via the SAFE website, conceded by the DOJ to the D.C. District Court.¹⁴

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 105-60.402-2(c); § 552(a)(6)(E)(vi).

Request for “News Media” Fee Status and Fee Waiver

EPIC is a “representative of the news media” for fee classification purposes. *EPIC v. Dep’t of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC’s status as a “news media” requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II); 41 C.F.R. § 105-60.305-10(d)(2).

Further, any duplication fees should also be waived because disclosure of the requested information “would contribute significantly to public’s understanding of the operations or activities of the Government and would not be primarily in the commercial interest” of EPIC. § 105-60.305-13; § 552(a)(4)(A)(iii). The GSA evaluates four considerations to determine whether this standard is met: (1) “Whether the subject of the requested records concerns ‘the operations or activities of the Government,’” (2) “Whether the disclosure is ‘likely to contribute’ to an understanding of Government operations or activities,” (3) “Whether disclosure of the requested information will contribute to [the] ‘public’s understanding,’” and (4) “Whether the requester has a commercial interest that would be furthered by the requested disclosure; and if so: whether the magnitude of the identified commercial interest of the requester is sufficiently large, in comparison with the public’s interest in disclosure, that disclosure is ‘primarily in the commercial interest of the requester.’” § 105-60.305-13(a)(1-4). EPIC’s request satisfies these four GSA considerations for granting a fee waiver. § 105-60.305-13(a)(1-4).

First, disclosure of the requested GSA records concerning Arkansas transfer of voter data following PACEI’s June 28th request self-evidently concerns “the operations or activities of the Government.” § 105-60.305-13(a)(1). This request involves a direct request from a presidential commission to a state officials to obtain state voter information, and the transfer of data to a federal website following that request.

Second, “disclosure is ‘likely to contribute’ to an understanding of Government operations or activities.” § 105-60.305-13(a)(2). The requested information about the Arkansas data transfer is

¹³ See Letter from Kris Kobach to Elaine Marshall, *supra* note 1.

¹⁴ Transcript of Temporary Restraining Order at 40, *supra* note 3.

not “already in the public domain.” *Id.* Few details surrounding the transfer have been disclosed to the public, and the existence of the transfer was first made public mere days ago.

Third, “disclosure of the requested information will contribute to [the] ‘public’s understanding” § 105-60.305-13(a)(3). As stated in the GSA FOIA regulations, the “identity and qualifications of the requester should be considered to determine whether the requester is in a position to contribute to public’s understanding through the requested disclosure.” *Id.* As already indicated, EPIC is a news media requester. EPIC regularly disseminates information obtained through the FOIA as a part of its public interest mission through website EPIC.org, a bi-weekly “EPIC Alert,” and other publications.¹⁵

Fourth, EPIC has no “commercial interest that would be furthered by the requested disclosure.” § 105-60.305-13(a)(4). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.¹⁶

For these reasons, a fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your decision concerning EPIC’s request for expedited processing within five working days. 41 C.F.R. § 105-60.402-2(d). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s/ Eleni Kyriakides

Eleni Kyriakides
EPIC Law Fellow

¹⁵ *About EPIC*, EPIC.org, <http://epic.org/epic/about.html>.

¹⁶ *Id.*



Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
<https://epic.org>

VIA E-Mail

July 12, 2017
Presidential Advisory Commission on Election Integrity
ElectionIntegrityStaff@ovp.eop.gov

Dear Sir or Madam:

This letter constitutes a request under the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center (“EPIC”) to the Presidential Commission on Election Integrity (the “Commission”).

EPIC seeks records in possession of the agency concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 Commission letter.

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

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.¹

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.² Further, the letter from the Commission indicated no familiarity with the data that may be disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

Following the proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that

¹ See, e.g. Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), <https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html>.

² Lewis Decl. Ex. 11., *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017).

Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.³

The Arkansas Secretary of State's Office charges \$2.50 per statewide voter registration data file.⁴ A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.⁵ The Office provides three types of files, with three clearly defined sets of information:

(1) "...Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."

(2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And

(3) "...a combination of the Voter Registration and Vote History files (VRVH)."⁶

The files are provided in ".CSV format" and "are available in CD format for pickup at the State Capitol Building or by mail" or "can also be placed on an FTP site."⁷

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

- (1) All records indicating payment by the Commission to obtain Arkansas voter records;
- (2) The completed "Data Request Forms," prepared by the Commission to obtain the Arkansas state vote records;
- (3) All records indicating the types of data transferred by Arkansas to the Commission; and
- (4) All records indicating the Commission's compliance with the Arkansas procedures to obtain state voter records.

³ Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

⁴ *Arkansas Voter Registration Data*, Arkansas.gov <http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf> (last visited July 12, 2017).

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

Request for Expedition

EPIC is entitled to expedited processing of this FOIA request. To warrant expedited processing, a FOIA request must concern a “compelling need.” 5 U.S.C. § 552(a)(6)(E)(i). “Compelling need” is demonstrated where the request is (1) “made by a person primarily engaged in disseminating information,” with (2) “urgency to inform the public concerning actual or alleged Federal Government activity.” § 552(a)(6)(E)(v)(II). This request satisfies both requirements.

First, EPIC is an organization “primarily engaged in disseminating information.” § 552(a)(6)(E)(v)(II). As the Court explained in *EPIC v. DOD*, “EPIC satisfies the definition of ‘representative of the news media.’” 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

Second, there is an “urgency to inform the public about an actual or alleged Federal Government activity.” § 552(a)(6)(E)(v)(II). The “actual...Federal Government activity” at issue PACEI’s request to states for detailed voter history information, conceded by PACEI in letters to the states,⁸ and the transfer of Arkansas voter data to PACEI via the SAFE website, conceded by the DOJ in D.C. District Court.⁹

“Urgency” to inform the public about the Arkansas voter data transfer to the SAFE website, following the Commission’s June 28th request. On June 28, 2017, PACEI independently requested that fifty states and D.C. - within approximately *ten business days* – disclose sensitive, personal information individuals are often required to provide to be eligible to vote. Since that date, public interest in the PACEI’s demand for state election officials to transfer personal voter data has dominated the news cycle, driven by prompt dissent of state officials in at least two dozen states across the political spectrum and public outcry.¹⁰ Following PACEI’s request less than two weeks ago, “[t]en states noted at least a slight increase in citizen calls and emails, and some citizens inquired about the process to unregister to vote, or how to secure their personal information.”¹¹

On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.¹² There are approximately 1.7

⁸ See Letter from Kris Kobach to Elaine Marshall, *supra* note 1.

⁹ Transcript of Temporary Restraining Order at 40, *supra* note 3.

¹⁰ Philip Bump & Christopher Ingraham, *Trump Says States Are ‘Trying to Hide’ Things from His Voter Fraud Commission. Here’s What They Actually Say*, Wash. Post (July 1, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/?utm_term=.bd2ba9587f57.

¹¹ Dylan Wells & Saisha Talwar, *Some voters un-registering following Trump administration's data requests*, ABC News (July 11, 2017), <http://abcnews.go.com/Politics/voters-registering-trump-administrations-data-requests/story?id=48578555>.

¹² Transcript of Temporary Restraining Order at 40, *supra* note 3.

million registered voters in the state of Arkansas potentially implicated by this transfer.¹³ The Commission will hold its first meeting on July 19, 2017.¹⁴ Ahead of that meeting, the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

In submitting this detailed statement in support of expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. § 552(a)(6)(E)(vi).

Request for “News Media” Fee Status and Fee Waiver

EPIC is a “representative of the news media” for fee classification purposes. *EPIC v. Dep’t of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC’s status as a “news media” requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II).

Further, any duplication fees should also be waived because disclosure of the requested information “is in the public interest” because (1) “it is likely to contribute significantly to public understanding of the operations or activities of the government,” and (2) disclosure “is not primarily in the commercial interest” of EPIC. § 552(a)(4)(A)(iii).

First, disclosure of the requested PACEI records concerning the Arkansas voter data transfer “is likely to contribute significantly to public understanding of the operations or activities of the government.” § 552(a)(4)(A)(iii). The requested PACEI records self-evidently concerns “operations or activities of the government.” *Id.* This request involves a direct request from a presidential commission to a state officials to obtain state voter information, and the transfer of data to a federal website following that request. Disclosure of the PACEI records is also “likely to contribute significantly to public understanding” of the Commission’s activities because, the requested information about the Arkansas data transfer is not “already in the public domain.” *Id.* Few details surrounding the transfer have been disclosed to the public. Indeed, the existence of the transfer was first made public mere days ago. Any additional information about the circumstances of the data transfer would there “contribute significantly” to the public’s understanding of PACEI’s activities. *Id.*

Second, disclosure of the requested information is not “primarily in the commercial interest” of EPIC. § 552(a)(4)(A)(iii). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.¹⁵

For these reasons, a fee waiver should be granted.

¹³ *Registered Voters [As of 6/1/16]*, Arkansas.gov <http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf> (last visited July 12, 2017).

¹⁴ Meeting notice, 82 FR 31063 (July 5, 2017).

¹⁵ *About EPIC*, EPIC.org, <http://epic.org/epic/about.html>.

Conclusion

Thank you for your consideration of this request. I anticipate your decision concerning EPIC's request for expedited processing within ten calendar days. 5 U.S.C. § 552(a)(6)(E)(ii)(I). For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org.

Respectfully submitted,

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC Law Fellow



Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
<https://epic.org>

VIA MAIL

July 13, 2017

The Honorable Mark Martin
Secretary of State
ATTN: FOIA Officer
256 State Capitol
500 Woodlane Street
Little Rock, AR 72201

Dear Sir or Madam:

This letter constitutes a request under the Arkansas Freedom of Information Act Ark. Code Ann. § 25-19-105(a)(2)(A) (1967) to receive copies of records, and is submitted on behalf of the Electronic Privacy Information Center (“EPIC”) to the Office of Arkansas Secretary of State Mark Martin.

EPIC seeks records in possession of the Office concerning the transfer of voter data from the State of Arkansas to the Department of Defense following the June 28, 2017 Commission letter.

EPIC does not assert a claim to Arkansas records as a citizen of the state. § 25-19-105(a)(1)(A). Rather, EPIC urges the Secretary of State to publicly release the requested records in light of the profound public interest favoring release. “The generation that made the nation thought secrecy in government one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to.” *EPA v. Mink*, 410 U.S. 73, 105 (1973) (Douglas, W. dissenting) (quoting from *The New York Review of Books*, Oct. 5, 1972, p. 7). Transparency secures “informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.” *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). Here, EPIC seeks records concerning the Arkansas transfer of state voter data to the federal government in the pursuit of this overriding public interest.

Background

On June 28, 2017, the Vice Chair of the Commission attempted to collect detailed voter histories from all fifty states and the District of Columbia. In letters to state officials, the Commission requested:

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.¹

The letter provides no indication that the Commission will pay fees for the receipt voter data. The Commission also indicated a website for the transmission of voter data, which has since been determined to be insecure for the receipt of personally identifiable information from the general public.² Further, the letter from the Commission indicated no familiarity with the data that may be disclosed by a particular state that received the request or the procedures the Commission would be required to follow to obtain voter data from a particular state.

Following the proceeding brought by EPIC, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017) on July 7, 2017 the U.S. Department of Justice told the D.C. District Court that Arkansas transferred voter data, to the Department of Defense's SAFE Website, following the letter from the Vice Chair.³

The Arkansas Secretary of State's Office charges \$2.50 per statewide voter registration data file.⁴ A requesting party also completes a "Data Request Form" in order to obtain the file and must mail payment (in check or money order form) to the Arkansas Secretary of State offices.⁵ The Office provides three types of files, with three clearly defined sets of information:

(1) "...Voter Registration (VR) file which is a list of all registered voters within the state. The file contains the Voter ID #, county of residence, voter name, address information (residential and/or mailing), phone number, DOB, precinct information, district information, party (if applicable) and the date last voted."

(2) "Vote History information for the state. This file lists the Voter ID # and Vote History data for all Federal elections from 1996 – current election cycle" while "older elections are incomplete since some counties did not enter voter results into the previously used VR databases." And

(3) "...a combination of the Voter Registration and Vote History files (VRVH)."⁶

¹ See, e.g. Letter from Presidential Advisory Commission on Election Integrity to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), <https://www.documentcloud.org/documents/3881856-Correspondence-PEIC-Letter-to-North-Carolina.html>.

² Lewis Decl. Ex. 11., *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017).

³ Transcript of Temporary Restraining Order at 40, *EPIC v. Commission*, No. 17-1320 (D.D.C. filed July 3, 2017).

⁴ *Arkansas Voter Registration Data*, Arkansas.gov

<http://www.sos.arkansas.gov/elections/Documents/Data%20Request%20Form.pdf> (last visited July 12, 2017).

⁵ *Id.*

⁶ *Id.*

The files are provided in “.CSV format” and “are available in CD format for pickup at the State Capitol Building or by mail” or “can also be placed on an FTP site.”⁷

EPIC seeks four categories of records from the agency concerning the Arkansas transfer of data to the Commission.

Records Requested

- (1) All records indicating payment by the Commission to obtain Arkansas voter records;
- (2) The completed “Data Request Forms,” prepared by the Commission to obtain the Arkansas state vote records;
- (3) All records indicating the types of data transferred by Arkansas to the Commission; and
- (4) All records indicating the Commission’s compliance with the Arkansas procedures to obtain state voter records.

Request for Fee Waiver

EPIC requests that copies of the records “be furnished without charge or at a reduced charge” because (1) the records “have been requested primarily for noncommercial purposes,” and (2) “waiver or reduction of the fee is in the public interest.” § 25-19-105(d)(3)(A)(iv).

First, disclosure of the records “have been requested primarily for noncommercial purposes. § 25-19-105(d)(3)(A)(iv). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.⁸

Second, “waiver or reduction of the fee is in the public interest.” § 25-19-105(d)(3)(A)(iv). The requested records concern a matter of profound public interest: the transfer of Arkansas voters’ data a Presidential commission. Nonetheless, there are few public details about the circumstances surrounding the transfer, and, indeed, the mere fact of the transfer was first made public only days ago.⁹ On July 7th, in a hearing before the D.C. District Court, the DOJ first revealed that Arkansas alone had transferred personal data to the Commission.¹⁰ There are approximately 1.7 million registered voters in the state of Arkansas potentially implicated by this transfer.¹¹ The Commission will hold its first meeting on July 19, 2017.¹² Ahead of that meeting,

⁷ *Id.*

⁸ *About EPIC*, EPIC.org, <http://epic.org/epic/about.html>.

⁹ Transcript of Temporary Restraining Order at 40, EPIC v. Commission, No. 17-1320 (D.D.C. filed July 3, 2017).

¹⁰ *Id.*

¹¹ *Registered Voters [As of 6/1/16]*, Arkansas.gov

<http://www.sos.arkansas.gov/elections/Documents/ARRegisteredVoters6-1-16.pdf> (last visited July 12, 2017).

the public must know whether the Commission and Arkansas state officials complied with state procedures in transferring this sensitive personal data.

For these reasons, a full fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. For questions regarding this request I can be contacted at 202-483-1140 x111 or FOIA@epic.org, cc: Kyriakides@epic.org. EPIC anticipates your response within a maximum of three working days. § 25-19-105(e).

EPIC requests receipt of responsive records via e-mail, and, if not “readily convertible” to electronic format, in physical copies via mail to the 1718 Connecticut Ave. NW, Suite 200, Washington, DC 20009. § 25-19-105(d)(2)(B).

Respectfully submitted,

/s/ Eleni Kyriakides

Eleni Kyriakides

EPIC Law Fellow

¹² Meeting notice, 82 FR 31063 (July 5, 2017).