

# **Exhibit 1**

# Presidential Documents

## Title 3—

## Executive Order 13799 of May 11, 2017

### The President

### Establishment of Presidential Advisory Commission on Election Integrity

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

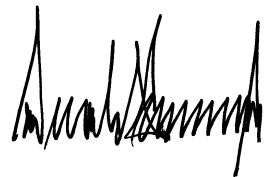
(e) Nothing in this order shall be construed to impair or otherwise affect:

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

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

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

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



THE WHITE HOUSE,  
May 11, 2017.

# **Exhibit 2**



the WHITE HOUSE



From the Press Office

[Speeches & Remarks](#)

[Press Briefings](#)

**[Statements & Releases](#)**

[Nominations & Appointments](#)

[Presidential Actions](#)

[Legislation](#)

[Disclosures](#)

## The White House

Office of the Vice President

For Immediate Release

June 28, 2017

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

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

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

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

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

[HOME](#)[BRIEFING ROOM](#)[ISSUES](#)[THE ADMINISTRATION](#)[PARTICIPATE](#)[1600 PENN](#)[USA.gov](#)[Privacy Policy](#)[Copyright Policy](#)

# **Exhibit 3**



---

## 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

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](mailto: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

# **Exhibit 4**

**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.<sup>1</sup> 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

---

<sup>1</sup>The 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 (11<sup>th</sup> 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 (11<sup>th</sup> 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 (11<sup>th</sup> 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 (11<sup>th</sup> 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.<sup>2</sup> 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**.

---

<sup>2</sup>The 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),<sup>3</sup> arguing that the VA failed to enforce this subsection in the numerous ways listed in their complaint.<sup>4</sup> Joint Status Report ("JSR"), at 10-11 (doc. 56). The plaintiffs then

---

<sup>3</sup>5 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."

<sup>4</sup>Plaintiffs 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 (7<sup>th</sup> 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 VBHCITA<sup>5</sup> 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

---

<sup>5</sup>The 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 statute<sup>6</sup> *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

---

<sup>6</sup>In 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.<sup>7</sup> 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.<sup>8</sup> 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

---

<sup>7</sup> 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).

<sup>8</sup>The 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.

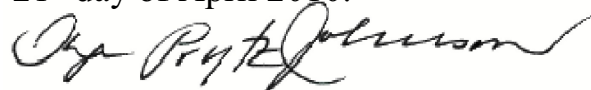
by various combinations of seven fields of identifying information. *Id.* at 9. The health care providers are identified on the hard drive by different combinations of forty-eight different fields of data. *Id.* at 10. All of this information was on a single external hard drive lost during a single data 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 21<sup>st</sup> day of April 2010.



---

INGE PRYTZ JOHNSON  
U.S. DISTRICT JUDGE

# **Exhibit 5**

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 "J. Bolten", is placed to the right of the typed 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](mailto: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.<sup>1</sup>
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).<sup>2</sup>
3. *Information technology (IT)* - means, as defined in the Clinger-Cohen Act<sup>3</sup>, 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 Act<sup>4</sup>, 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.*<sup>5</sup>

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),<sup>6</sup>
  - 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 controls<sup>7</sup>); 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](mailto:PIA@omb.eop.gov) along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300<sup>8</sup>); 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 assessment<sup>9</sup>. 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)*<sup>10</sup>.

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 Statement<sup>11</sup>;
    - ii. a description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement<sup>12</sup>;
    - iii. a statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement<sup>13</sup>;
    - 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 Act<sup>14</sup>.
  - 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*<sup>15</sup>. 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*<sup>16</sup>. 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](http://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 Policy<sup>18</sup>.
      - 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)<sup>19</sup>.
      - 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)<sup>20</sup>.
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*<sup>21</sup>. Agencies should continue to comply with existing requirements for computer security in administering their websites<sup>22</sup> 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 call<sup>23</sup>.

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.

# **Exhibit 6**



## 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

# **Exhibit 7**

## DECLARATION OF NAME

I, Kimberly Bryant, declare as follows:

1. My name is Kimberly Bryant. I am over 18 years old. The information in this declaration is based on my personal knowledge.

2. I am a resident San Francisco, CA.

3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.

4. EPIC is a non-profit, public interest research center in Washington, DC.

EPIC 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. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - [epic.org](http://epic.org).

5. I am currently registered to vote in California.



6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017

Kimberly Bryant  
NAME

# **Exhibit 8**

## DECLARATION OF Julie E. Cohen

I, Julie E. Cohen, declare as follows:

1. My name is Julie E. Cohen. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident of Bethesda, MARYLAND.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC 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. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - [epic.org](http://epic.org).
5. I am currently registered to vote in MARYLAND.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017

  
Julie E. Cohen

# **Exhibit 9**



## DECLARATION OF William T. Coleman III

I, William T. Coleman III, declare as follows:

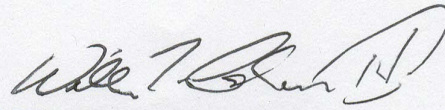
1. My name is William T. Coleman III. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Los Altos, California.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC 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. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - [epic.org](http://epic.org).
5. I am currently registered to vote in Los Altos, California.



6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017



---

William T. Coleman III

# **Exhibit 10**



## DECLARATION OF Harry R. Lewis


I, Harry R. Lewis, declare as follows:

1. My name is Harry R. Lewis. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Brookline, Massachusetts.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC 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. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - [epic.org](http://epic.org).
5. I am currently registered to vote in Massachusetts.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017

  
\_\_\_\_\_  
Harry R. Lewis

# **Exhibit 11**

## DECLARATION OF PABLO GARCIA MOLINA

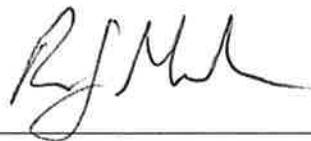
I, **PABLO GARCIA MOLINA**, declare as follows:

1. My name is **PABLO GARCIA MOLINA**. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident of WASHINGTON, DC.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC 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. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - [epic.org](http://epic.org).
5. I am currently registered to vote in DC.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017



---

PABLO GARCIA MOLINA

# **Exhibit 12**

DECLARATION OF NAME

(Peter G Neumann)

I, Peter G. Neumann declare as follows:

1. My name is Peter G. Neumann. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Palo Alto, California.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC 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. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in California.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017

Peter G Neumann



7/5/2017



# **Exhibit 13**

## DECLARATION OF BRUCE SCHNEIER

I, Bruce Schneier, declare as follows:

1. My name is Bruce Schneier. I am over 18 years old. The information in this declaration is based on my personal knowledge.

2. I am a resident of Minneapolis, Minnesota.

3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.

4. EPIC is a non-profit, public interest research center in Washington, DC.

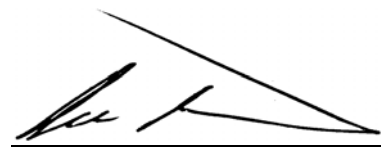
EPIC was established to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - [epic.org](http://epic.org).

5. I am currently registered to vote in Minnesota.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017

A handwritten signature in black ink, appearing to read 'Bruce Schneier', written over a horizontal line.

Bruce Schneier

# **Exhibit 14**

## DECLARATION OF James Waldo

I, James Waldo, declare as follows:

1. My name is James Waldo. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Dracut, Massachusetts.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC 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. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - [epic.org](http://epic.org).
5. I am currently registered to vote in Massachusetts.

6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017

  
James Waldo

# **Exhibit 15**

## DECLARATION OF Shoshana Zuboff

I, Shoshana Zuboff, declare as follows:

1. My name is Shoshana Zuboff. I am over 18 years old. The information in this declaration is based on my personal knowledge.
2. I am a resident Nobleboro, Maine.
3. I am a member of the Electronic Privacy Information Center (EPIC) advisory board. I joined EPIC because I am concerned about protecting privacy, freedom of expression, and democratic values in the information age.
4. EPIC is a non-profit, public interest research center in Washington, DC. EPIC 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. EPIC routinely files comments with federal agencies advocating for improved privacy standards and rules. EPIC works closely with a distinguished advisory board, with expertise in law, technology and public policy. EPIC maintains one of the most popular privacy web sites in the world - epic.org.
5. I am currently registered to vote in Maine.



6. I do not consent to the collection of my personal data by the Commission recently created by the President of the United States.
7. The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm.

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

Executed July 5, 2017

Shoshana Zuboff

Shoshana Zuboff

# **Exhibit 16**



NCSL

# THE CANVASS

STATES AND ELECTION REFORM®



Issue 66 | February 2016

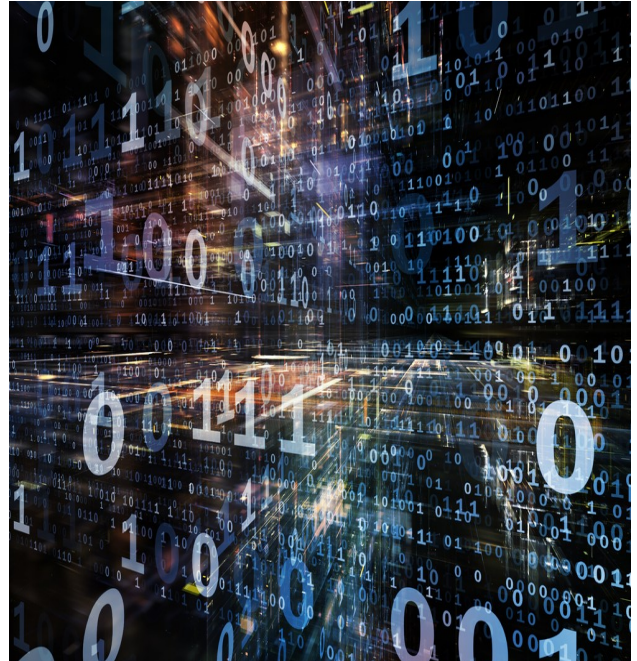
canvass (n.)

Compilation of election returns and validation of the outcome that forms the basis of the official results by a political subdivision.

—U.S. Election Assistance Commission: *Glossary of Key Election Terminology*

## It's a Presidential Election Year: Do You Know Where Your Voter Records Are?

One of the secrets of the election world is how readily available voter data can be—and it's been making headlines lately. In late 2015, information such as name, address, party, and voting history relating to **approximately 191 million voters was published online**. And recently, the presidential campaign of Texas Senator Ted Cruz came under fire for a mailer in Iowa that **used voter data to assign grades to voters** and compared them to neighbors to motivate turnout. Voter records have always been public information, but now it's being used in new ways. Here are some key facts you need to know about the privacy (or lack of privacy) of voter information.



### *What voter information is public record?*

All 50 states and the District of Columbia provide access to voter information, **according to the U.S. Elections Project** run by Dr. Michael McDonald at the University of Florida; but as with everything related to elections there are 51 different variations on what information is provided, who can access it, and how much it costs to get it.

Generally, all states provide the name and address of the registered voter. From there it gets complicated. Some states have statutory limitations on what information is available. At least 25 states limit access to social security numbers, date of birth or other identifying factors such as a driver's license number. Ten states limit the contact information, such as a telephone number or email address. Nine states include miscellaneous information like place of birth, voter identification numbers, race, gender, secondary addresses, accommodations to vote and signatures on the list of exemptions for the voter file. Texas **specifically restricts the residential address** of any judge in the state.

While, there are 13 states that have no codified restrictions on the information available to the public, the secretary of state may have the ability to limit information. Six states have a general prohibition on "information of a personal nature" or information related to matters of individual safety that pertain to voter records as well as all other state records.

Every state except Rhode Island as well as the District of Columbia also provide information about voter history—not who a person voted for but just if they voted (Rhode Island does not provide access to that information). Absentee voting information—ballot requests or permanent absentee lists—are also available, sometimes for an extra fee and sometimes only through municipalities or local jurisdictions. At least five states do not offer absentee voting data as part of the available voter file.

### Inside this Issue

- It's a Presidential Election Year: Do You Know Where Your Voter Records Are? **1**
- One Big Number **3**
- Election Legislation By the Numbers: 2015 and 2016 **4**
- Ask NCSL **4**
- From the Chair **5**
- The Election Administrator's Perspective **5**
- Worth Noting **6**
- From NCSL's Elections Team **6**

TO SUBSCRIBE to *The Canvass*, please email a request to [TheCanvass@ncsl.org](mailto:TheCanvass@ncsl.org)

(cont. on page 2)



(Voter Records, cont. from page 1)

## Who can access the information?

All states allow candidates for elected offices or political parties to access voter records, typically for political purposes. Which makes sense—if you want to run for office it helps to have a list of your constituents to contact.

Beyond candidates and political parties, who can access voter lists varies state by state. Eleven states do not allow members of the public to access voter data. Several other states restrict access to state residents (11), other registered voters (7), non-profit organizations (6), and those doing research (9).



## What can it be used for?

Most often, voter information can be used for “non-commercial” purposes only—in other words, an entity or person can’t access the information to sell a product or a service, but can use it for anything else.

Several states are stricter, limiting the use to just political purposes or election purposes, which may or may not include voter registration drives, getting-out-the-vote and research. Further, the available uses may vary between the different users groups mentioned above. And it can be hard for states to control what happens to the data once it’s been turned over.

## Cost for accessing data

Accessing voter data comes with a price. “There is a wide variation in the costs that states charge for accessing this information,” says McDonald.

Washington, D.C. only charges \$2 for the entire voter registration list; other bargain rates include Arkansas (\$2.50) and New Jersey (\$2.55).

In Massachusetts, New York, Ohio, Oklahoma, Vermont, Washington or Wyoming accessing the voter is free, provided you meet the criteria.

Accessing the data is much pricier in some states. Several states charge \$5,000 and Wisconsin charges \$12,500. Alabama and Arizona got creative with setting their fees by charging one cent per voter, resulting in a cost of upwards of \$30,000.

Ultimately, the average cost for a voter list is approximately \$1,825—which isn’t prohibitively expensive.

## What other exceptions are there?

As mentioned above, states can restrict certain information from being released in the voter file. But states can also withhold information if a voter’s information is marked as confidential.

## Voter-Shaming—How does Social Pressure Influence Voter Turnout?

Get ready to add “voter-shaming” to your vocabulary. The term has been popping up in news stories everywhere over the past month—most notably in controversial presidential campaign mail pieces that compared the voting history of Iowa voters to their neighbors. But just what is it exactly?



The practice of comparing voting history to that of peers stems from a 2008 study conducted by Alan Gerber and Donald Green from Yale University and Christopher Larimer from the University of Northern Iowa entitled [Social Pressure and Voter Turnout: Evidence from a Large Scale Field Experiment](#).

The study examined the effect of various mailings on voter turnout. Specifically, the mailers had different messages that encouraged voters to do their civic duty, indicated that the voter’s vote history was being studied, listed the vote history of each member of the household, or listed the voter’s vote history compared to their neighbors. The results showed that each of these “social pressures” increased voter turnout but none more so than the neighbor mailing which increased turnout by eight percent.

Candidates, campaigns and other researchers took notice of the study which has resulted in “voter-shaming” mailers popping up in places like [Alaska](#), [North Carolina](#) and most recently in the first two presidential nominating contests in the nation—Iowa and [New Hampshire](#). They’ve shown to be powerful motivators so keep an eye out for social pressure mailers coming soon to your mailbox.

Thirty-nine states maintain address confidentiality programs designed to keep the addresses of victims of domestic violence or abuse, sexual assault or stalking out of public records for their protection. The programs allow victims to use an alternate address, usually a government post office box, in place of their actual home address. Of those 39 states, at least 29 of them have specific references to voter registration and voter records. That means those voter records won’t be included in the comprehensive list purchased from the state.

In 2015, Iowa established an [address confidentiality program that includes voter records](#) and Florida updated their [address confidentiality law](#) to include victims of stalking. This year [Kentucky](#) and [New York](#) have legislation to connect address confidentiality to voter records.

Another sensitive demographic is 16- and 17 year-olds that may be able to preregister under state law. How do you protect the information of minors? Of course the answer is complicated. Utah considers the records of preregistered voters private under

(cont. on page 3)



(Voter Records, cont. from page 2)

state law and Minnesota designates preregistered voters as “pending” until they become eligible in which case they are changed to “active.” Only active voters are included on the public voter list. The same is true in Louisiana, Missouri, New Jersey and Rhode Island.

In states where 17-year-olds are on the active voter rolls because they’ll be able to vote in the next election, their information will be treated like all the other voters. That’s the case in Nebraska where 17-year-olds can register, and in some cases vote, if they turn 18 by the first Tuesday after the first Monday in November. Maine doesn’t allow the public to access the voter list, but since the Pine Tree State allows 17-year-olds who will be 18 by the general election to vote in primaries, that information is included on the lists accessible to candidates and political parties. Delaware, Iowa, Nevada and Oregon have similar systems in which those under 18 are included on the list if they turn 18 by the date of the general election or are eligible to vote in primaries. Florida includes the information of preregistered voters unless an exemption is claimed.

### How have legislatures responded?



Sen. Paul Doyle (CT)

In 2015, 16 bills in 12 states were introduced that dealt with some aspect of distribution and the availability of voter information. In Connecticut, Senator Paul Doyle (D) responded to constituent concerns about their voter information being publicly available online by filing legislation to specifically prohibit that information from being **published on the Internet**. “My constituent told me that they were going to take themselves off the voter list and de-register because of their information

being available online—that’s a problem,” says Doyle. “I understand First Amendment concerns, but I wanted to start the discussion on the issue.”

Three bills were enacted in 2015. In addition to the Florida and Iowa bills mentioned above, Alabama **decided to allow state legislators to receive only one free copy** of the voter list for their district rather than two.

So far in 2016, there are 13 bills in 8 states—some carried over from last year—dealing with voter information and a few those

are carryovers from 2015. One of the more notable battles is being waged in Florida where Senator Thad Altman (R) has **introduced legislation** to make voters’ residential addresses, dates of birth, telephone numbers and email addresses confidential and only available to candidates, political parties and election officials, and not to the public. Senator Altman’s bill also seeks to protect all the personal information of 16- and 17-year-olds who preregister to vote. The bill has the **support** of the Florida State Association of Supervisors of Elections.



Sen. Thad Altman (FL)

“Right now all this data is public information,” says Altman. “You can put it on the Internet or resell it. You can see someone’s address, phone number, and party affiliation. There have been cases where someone received an electioneering piece that said how many times they voted. I’m concerned it could keep people from voting or registering to vote or lead to discrimination. If you want that information to be private you should have that right.”

Other states are tackling this issue as well. **West Virginia** is considering legislation to keep private the address of law enforcement officers and their families. Massachusetts is one of the states that offers voter information for free, but now has legislation to **limit public access and to charge for lists**. Legislation in Kentucky seeks to **remove social security numbers** from the voter list. Lastly, Illinois wants to make sure you know who paid for voter information on **any mailings that use your voter history**.

But there are some who are concerned states may go too far in limiting access to this information. “I’m a researcher who studies voting trends to improve elections—I need access to this information,” says McDonald. “There has to be a balance between privacy concerns and access.”

Given some of the recent headlines, it remains to be seen how states will react to the increased concern of voter privacy. It’s the information age where answers are available at the click of a button and that includes voter information.

### One big number

**144 million**

**144 million.** The approximate number of eligible American voters that did not vote in the 2014 elections according to data from the U.S. Elections Project and quoted by **The Pew Charitable Trusts’ David Becker in the Stanford Social Innovation Review**. It’s one of a 15-part series called “Increasing Voter Turnout: It’s Tougher Than You Think.”

Becker calls for a two part approach. First—conduct research; more specifically “comprehensive surveys of the eligible electorate that never or rarely votes to assess the attitudes and behaviors of these potential voters.” Then “create field experiments that test the effectiveness of various messages and modes of contact on nonvoters, maintaining a randomized control group that would receive no encouragement to vote.” The end result could be a “toolkit for those seeking to engage citizens in the democratic process to reach potential voters in a highly efficient, cost-effective way.”





# Election Legislation By the Numbers: 2015 and 2016

Election years are notoriously stodgy when it comes to enacting election legislation. First, a recap of 2015:

- 2,355 election-related bills were introduced.
- 241 bills in 45 states were enacted.
- 17 bills in seven states were vetoed.

Highlights included online voter registration, automatic voter registration and items related to preparing for the presidential election. For more information on what exactly was enacted in each states visit [NCSL's 2015 Elections Legislation Enacted by State Legislatures](#) webpage.

Now onto 2016:

- 1,747 election-related bills have been introduced in 42 states, including some bills from 2015 that were carried-over into 2016.
- Ten bills have been enacted already including: one in Michigan that **eliminates straight-ticket voting**; one in New Hampshire that allows **local selectman to appoint a replacement** if they can't fulfill their duties on election; four in New Jersey, which allow **preregistration for 17-year-olds**, **standardize polling place hours** and deal with other administrative issues; two in South Dakota including **authorizing the use of vote centers and electronic pollbooks statewide**; and one in West Virginia concerning **candidate withdrawal from the ballot**.
- Automatic voter registration seems to be leading the pack this year with a big increase in legislation from 2015. So far in 2016, 88 bills in 27 states have been introduced which is a 25 percent increase from last year.

- **Voter ID** legislation continues to be common, with 74 bills introduced so far and Missouri **poised to join the ranks** of strict voter ID states.
- **Absentee voting** issues remains popular with 68 bills pending and several states looking at early voting or no-excuse absentee voting.



- Because **online voter registration** is now active or authorized in 32 states plus the District of Columbia, legislation on this has taken an expected dip. Only 16 bills are in the hopper, but with high profile states like Ohio and Wisconsin considering enacting systems, online voter registration will remain a hot topic.

- Other registration issues, like preregistration for youth, **same day registration** and **list maintenance**, are still hot topics with a combined 129 bills.

- 179 bills deal with poll workers, polling places and vote centers.
- 134 bills deal with some aspect of the **primary process**.
- **Voting equipment** and technology bills total 53.
- 68 bills address election crimes.

NCSL's [Elections Legislation Database](#) is your go-to resource for all things 2016 election legislation. Stay tuned for updates throughout the year.



## *How many states allow a candidate to withdraw from the ballot after already qualifying?*

All but six states allow candidates to withdraw after making it onto the ballot. This is generally subject to some exceptions, most often deadlines after which a candidate may not withdraw. These deadlines are usually well in advance of the election, but in some states the deadline is much closer to the election. For example, in Alabama a candidate may withdraw even after ballots have been printed for the election. In Arizona, Georgia, Hawaii, Maine, Ohio, and Wyoming candidates may withdraw after ballots have been printed, but election officials must post notice of the withdrawal in prominent locations in polling places. Only California, Kansas, New

Hampshire, and Wisconsin expressly prohibit candidates from withdrawing from the ballot. Utah and Tennessee do not specifically address candidate withdrawal in statute. In Kansas the rule isn't absolute: A candidate may withdraw from the ballot if they certify to the Secretary of State that they do not reside in Kansas. In New Hampshire, a candidate may not withdraw once they have received a nomination, but they may be disqualified for age, health, or residency reasons. In Wisconsin, the name of a candidate may be removed from the ballot only if the candidate dies before the election, although a candidate may refuse to take office after being elected. For the full list contact the elections team.



## From the Chair

Assembly Member Sebastian Ridley-Thomas serves as chairman of the Elections and Redistricting Committee in the California Assembly. He represents the 54th Assembly district which is entirely in Los Angeles County and consists of communities in the western part of the city of Los Angeles. Assembly Member Ridley-Thomas spoke to The Canvass on Feb. 24.

- “We’ve done a great deal on language access, accessibility for those with special needs and engaging our high school students and young people through preregistration and other means. The new motor voter law will help to add potentially 5 million people to the voter rolls, but now they have to turn out to vote.”
- “We are working with several groups on legislation to give special districts more flexibility in transitioning from at-large representation to district-based representation ([AB 2389](#)). Currently, these special districts can only make this change after receiving approval from the voters. Enabling them to do it by ordinance will save time and money, especially in court costs, and help to de-escalate the tension in the courts. The residents will be better represented through this method. Communities are better served when they can elevate members of their own choosing that reflect them and their priorities.”
- “Myself and Senator Ben Allen (chair of the Senate Committee on Elections and Constitutional Amendments) are among the youngest legislators and we are focused on the future, but also not leaving our peers behind. I’m proud that California is looking toward the future and making elections better and more collaborative so voters can express their will and values at the ballot box. California is the innovation hub of the world and there’s no reason that can’t apply to elections.”

Read the [full interview](#) with Assembly Member Ridley-Thomas.



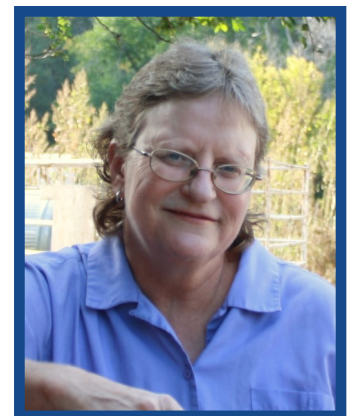
*Assembly Member  
Sebastian Ridley-Thomas*

## The Election Administrator’s Perspective

Sue Ganje serves as the auditor for Fall River County and Oglala Lakota County (formerly Shannon County) in southwest South Dakota. She is one of two auditors in South Dakota that cover multiple counties; Oglala Lakota County doesn’t have a county seat, so the administrative offices are in Fall River County. Ganje spoke to The Canvass on Feb. 18.

- “Things have definitely changed. I can remember hand-counting ballots into the early morning hours and using different colored ballots and straight party voting for political parties. When I look at where we were then to where we are now—we’ve come a long way in elections.”
- “I’m very interested in vote centers. Everywhere you go is a distance in our counties. There can be 30, 40 or sometimes 50 miles between towns. If a voter is not at the right location for voting at the time the polls close, they may have to vote a provisional ballot that may or not be counted. Vote centers would help alleviate that problem. Right now, the county cannot afford the equipment needed for a vote center but I hope there will be funding in the future.”
- “I’m proud that we’ve helped every voter we can to cast a vote. We have a great statewide voter registration system in South Dakota. It’s very easy for us to use and we have all the relevant county records right there in order to update the voter records. I think other states should be looking at our system to use.”
- “I think we also have a good voter identification system. The state created a personal identification affidavit that voters who do not have IDs can sign at the polls. It works well, and the voter can then vote a regular ballot, not a provisional one. The worst thing we want to do as election officials is turn someone away from the polls. Everyone gets to vote here.”

Read the [full interview](#) with Ganje.



*Fall River County/Oglala Lakota  
County Auditor Sue Ganje*



## Worth Noting

- The Maryland Legislature has overridden the veto of Governor Larry Hogan and [will now restore voting rights to felons](#) once they have completed their prison sentence. Previously felons waited until completing parole and probation to get voting rights restored.
- Voter ID is back in the news as the Missouri Senate [considers two measures to require voter identification](#). One is a constitutional amendment that would be sent to voters for their approval and the other would limit the types of identification that can be used. Both measures previously [passed the Missouri House](#).
- Speaking of voter ID, NPR has a [look at the issue along with the recent changes](#) made to the state instructions on the federal voter registration form by the U.S. Election Assistance Commission (EAC).
- Politico has an excellent piece on how the recent passing of Supreme Court Justice Antonin Scalia [could affect cases and court rulings related to elections and redistricting](#).
- The plan by the Virginia Republican Party to [require loyalty oaths for voters](#) in the Republican Presidential Primary has been scrapped after earning the ire of presidential candidate Donald Trump and others. The Old Dominion State has an open primary that lets independents participate.
- As online voter registration continues to gain steam in states, David Levine, an election management consultant, offers [five key steps to getting online voter registration right](#) in electionlineWeekly.
- Oregon, the first state in the country to have automatic voter registration, began implementing its program in January. The Beaver State has added [4,653 voters](#) to the rolls since the law took effect.
- Nebraska is the latest state grappling [with legislation allowing voters to take ballot selfies](#).
- A new year means a new look at why Americans [aren't yet voting over the Internet](#) or on their phones according to USA Today.
- New Mexico is [on the cusp of allowing 17-year-olds to participate in primary elections](#) if they will turn 18 by the general election.
- The uncertainty surrounding the boundaries for two North Carolina congressional districts [may have an impact on military and absentee voters](#) who have already begun early voting for the March primary.
- Straight-ticket voting could be as dead as the dodo in a few years—one of the few remaining states to allow the practice, Indiana, is [looking at eliminating it](#).
- The Election Law Program at William and Mary Law School has a series of [helpful video modules](#) on various election issues, like campaign finance, public access to voted ballots, voting equipment malfunctions and absentee ballot disputes.



Replacing outdated voting machines is one of the hottest topics in election news right now so keep an eye on NCSL's [Election Technology News Feed](#) for all the latest on election technology and funding from around the nation. The page collects news articles on purchases, and discussions about voting systems, electronic pollbooks or other major decisions, broken down by state.

The NCSL team has been hard at work updating several of our webpages to provide the most current information: [2016 State Primary Dates](#), [Online Voter Registration](#), [Voter ID](#), [Absentee and Early Voting](#), and [Provisional Ballots](#).

Thanks for reading, let us know your news and please [stay in touch](#).

—*Wendy Underhill and Dan Diorio*

*The Canvass*, an Elections Newsletter for Legislatures © 2015  
Published by the National Conference of State Legislatures  
William T. Pound, Executive Director

In conjunction with NCSL, funding support for *The Canvass* is provided by The Pew Charitable Trusts' Election Initiatives project.

Any opinions, findings or conclusions in this publication are those of NCSL and do not necessarily reflect the views of The Pew Charitable Trusts. Links provided do not indicate NCSL or The Pew Charitable Trusts endorsement of these sites.

TO SUBSCRIBE, contact [TheCanvass@ncsl.org](mailto:TheCanvass@ncsl.org)



# **Exhibit 17**

## SECOND DECLARATION OF Harry R. Lewis

I, Harry Lewis, declare as follows:

1. My name is Harry R. Lewis.
2. I am Gordon McKay Professor of Computer Science at Harvard University.

I have served on the faculty at Harvard for 44 years, a span which includes terms as Dean of the College and as interim Dean of the John A. Paulson School of Engineering and Applied Sciences.

3. I am the author of six books and numerous articles on various aspects of computer science, education, and technology.
4. I am a member of the Electronic Privacy Information Center (EPIC) advisory board.
5. On July 5, 2017, at approximately 6 pm EDT, I undertook to review the security of the website "safe.amrdec.army.mil," recommended by the Vice Chair of the Presidential Advisory Commission on Election Integrity in the letter of June 28, 2017 to state election officials, for the delivery of voter roll data.
6. This is the same website that the Vice Chair described in his July 5, 2017 declaration in this matter as "a secure method of transferring large files up to two gigabytes (GB) in size."

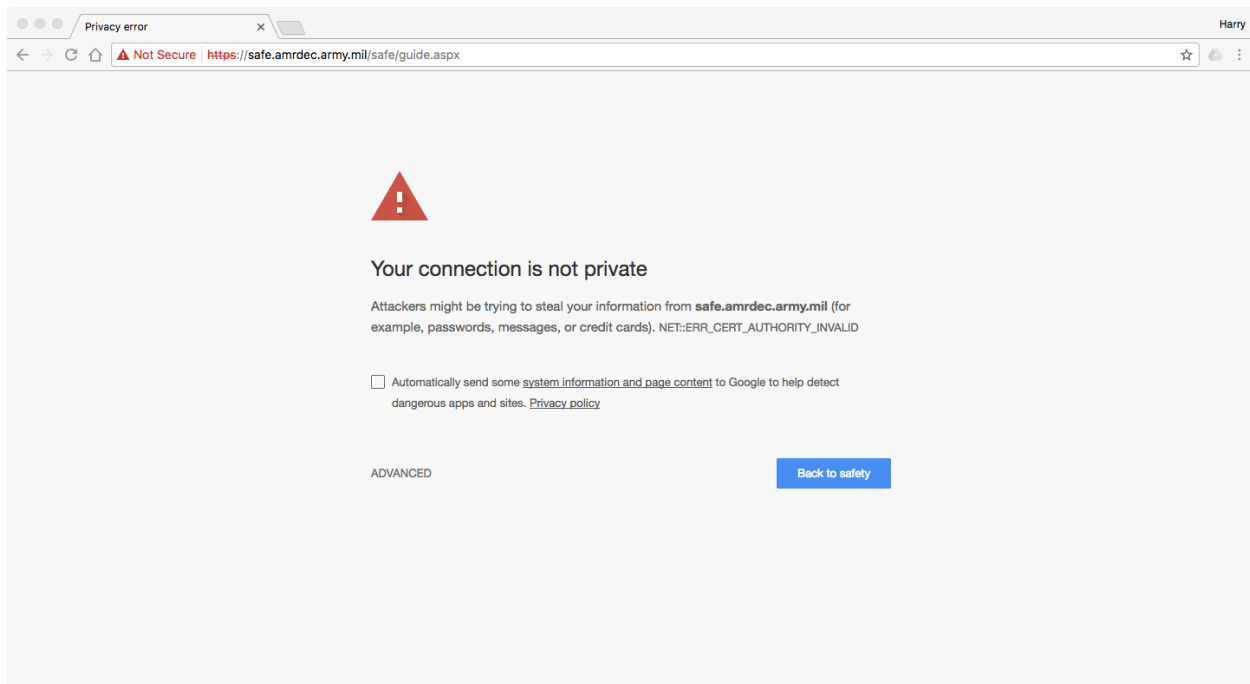
7. The Google Chrome browser returned an error message with a bright red warning mark, which stated, “Your connection is not private – Attackers might be trying to steal your information from **safe.amrdec.army.mil** (for example, passwords, messages, or credit cards).”
8. The Apple Safari browser returned an error message, which stated “Safari can’t verify the identity of the website ‘safe.amrdec.army.mil.’ The certificate for this website is invalid. You might be connecting to a website that is pretending to be ‘safe.amrdec.army.mil,’ which could put your confidential information at risk.”
9. It is my opinion that “safe.amrdec.army.mil” is not a secure website for the transfer of personal data.
10. I have attached to this affidavit contemporaneous screen shots of the responses from the Google Chrome browser and the Apple Safari browser I observed

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

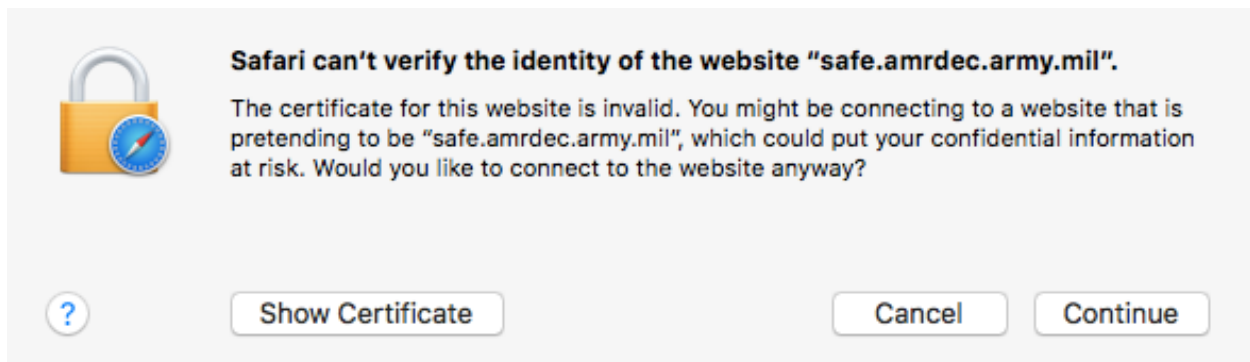
Executed July 5, 2017

  
\_\_\_\_\_  
Harry R. Lewis

## 1. Screen shot of Google Chrome browser message



## 2. Screen shot of Apple Safari browser message



# **Exhibit 18**



# 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](#)

# **Exhibit 19**





**U.S. ELECTION ASSISTANCE  
COMMISSION  
OFFICE OF INSPECTOR GENERAL**

**FINAL REPORT:**

**Audit of U.S. Election Assistance  
Commission's Compliance with  
Section 522 of the  
Consolidated Appropriations Act 2005**

**Report No.  
I-PA-EAC-04-12  
May 2013**



U.S. ELECTION ASSISTANCE COMMISSION  
Office of Inspector General

May 7, 2013

TO: Alice Miller,  
Acting Executive Director and Chief Operating Officer

FROM: Curtis W. Crider *Curtis W. Crider*  
Inspector General

SUBJECT: Review of the U.S. Election Assistance Commission Compliance with  
Section 522 of the Consolidated Appropriations Act 2005

We contracted with the independent certified public accounting firm of CliftonLarsonAllen, LLP to perform an audit of EAC's compliance with protection of personal data in an identifiable form. The audit included assessing compliance with applicable federal security and privacy laws and regulations as well as assessing the privacy and data protection procedures used by EAC as they relate to the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005. The contract required that the audit be performed in accordance with generally accepted government auditing standards. Attached is a copy of the final report.

In response to the draft report dated February 27, 2013, the EAC generally agreed with the report which included providing expected completion dates for each of the recommendations.

The legislation as amended, creating the Office of Inspector General (5 U.S.C. § App. 3) requires semiannual reporting to Congress on all inspection and evaluation reports issued, actions taken to implement recommendations, and recommendations that have been implemented. Therefore, a summary of this report will be included in our next semiannual report to Congress.

If you have any questions regarding this report, please call me at (202) 566-3125.

Copy to: Mohammed Maeruf, CIO  
Annette Lafferty, CFO  
Sheila Banks, PO

**U.S. ELECTION ASSISTANCE COMMISSION (EAC)**

**Report on the 2012 Review of EAC's Compliance with Section  
522 of the Consolidated Appropriations Act 2005**

**(Policies, Procedures & Practices of Personally Identifiable  
Information)**

**April 25, 2013**



CliftonLarsonAllen

CliftonLarsonAllen LLP  
www.cliftonlarsonallen.com

Mr. Curtis Crider  
Office of the Inspector General  
U.S. Election Assistance Commission  
1225 New York Avenue NW, Suite 1100  
Washington, DC 20005

Dear Mr. Crider,

We are pleased to present our report on the U.S. Election Assistance Commission's (EAC) compliance with protection of personal data in an identifiable form. This review included assessing compliance with applicable federal security and privacy laws and regulations as well as assessing the privacy and data protection procedures used by EAC as they relate to the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005. The objective of our review was to determine whether EAC's stated privacy and data protection policies and procedures for personal information of employees and the public are adequate and effective and in compliance with Section 522 of the Appropriations Act of 2005.

We interviewed key personnel involved in the identifying and protecting personally identifiable information and reviewed documentation supporting EAC's efforts to comply with federal privacy and security laws and regulations.

This audit was performed between November 2012 to January 2013 at the EAC office in Washington, District of Columbia. We conducted this performance audit with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We appreciate the opportunity to have served you once more and are grateful for the courtesy and hospitality extended to us by EAC personnel. Please do not hesitate to call me at (301) 931-2050 or email at [George.fallon@cliftonlarsonallen.com](mailto:George.fallon@cliftonlarsonallen.com) if you have questions.

Sincerely,

CLIFTONLARSONALLEN LLP

Calverton, Maryland  
April 25, 2013

## Table of Contents

<b>Executive Summary</b> .....	1
<b>Introduction</b> .....	1
<b>Scope and Methodology</b> .....	2
<b>Audit Findings and Recommendations</b> .....	3
<b>Conclusions and Recommendations</b> .....	6
<b>Agency Response and OIG Comments</b> .....	7

## Executive Summary

Based upon our review, EAC has made improvements to strengthen controls over the security of Personally Identifiable Information (PII) including conducting Privacy Impact Assessments (PIA), appointed a senior agency official for privacy and privacy officer, and developed formalized policies and procedures for PII, however more work remains to be accomplished.

Specifically, EAC was not fully compliant with Section 522 of the Consolidated Appropriations Act 2005 requirements, including:

- Effective encryption mechanisms to appropriately protect agency information, including PII were not implemented;
- Formalized PII usage reports were not submitted to the Office of Inspector General (OIG); and
- EAC Records Management Processes and Procedures Standard Operating Procedures were not formally documented.

## Introduction

On December 8, 2004, the President signed into law H.R. 4818, *Consolidated Appropriations Act, 2005* (Public Law 108-447). Title V, Section 522 of this act mandates the designation of a senior privacy official, establishment of privacy and data protection procedures, a written report of the agency's use of information in an identifiable form,<sup>1</sup> an independent third party review of the agency's use of information in an identifiable form, and a report by the Inspector General to the agency head on the independent review and resulting recommendations. Section 522 (d) (3) requires the Inspector General to contract with an independent third party privacy professional to evaluate the agency's use of information in an identifiable form, and the privacy and data protection procedures of the agency. The independent review is to include (a) an evaluation of the agency's use of information in identifiable form, (b) an evaluation of the agency's privacy and data protection procedures, and (c) recommendations on strategies and specific steps to improve privacy and data protection management. Section 522 requires the agency to have an independent third party review at least every 2 years and requires the Inspector General to submit a detailed report on the review to the head of the agency. The third party report and the related Inspector General report are to be made available to the public, i.e. internet availability.

---

<sup>1</sup> Identifiable form is 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. Personally identifiable information (PII) has a similar meaning and will be the term used throughout this document.

## Scope and Methodology

Our audit objectives were to evaluate and report on whether the EAC had established adequate privacy and data protection policies and procedures governing the collection, use, disclosure, transfer, storage and security of information relating to agency employees and the public in accordance with Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005.

Our audit scope included the review of EAC documents, and a walkthrough of how PII data is received, processed and stored in electronic and manual form at EAC headquarters in Washington, DC. The following specific procedures were performed to complete the survey assessment:

- Issued a document request list detailing the initial information needed for the audit.
- Reviewed any baseline documentation prepared by EAC to gain a preliminary high level understanding of information in an identifiable form and its use throughout EAC.
- Identified key individuals with responsibility or control over privacy data collected, maintained or processed throughout EAC.
- Evaluated existing work performed by the EAC, the OIG or third parties.
- Reviewed all available documentation related to audits regarding the EAC's implementation and compliance with privacy policy, and practices.
- Coordinated administrative, technical and key logistical aspects of the audit with OIG.
- Obtained permission from the OIG and management to review working papers, documentation, and reports at agreed-upon dates, times and locations; and perform interviews as needed to establish an understanding of missing or incomplete support for the purposes of conducting the privacy audit.
- Obtained an understanding of EAC's privacy and data protection policies and procedures for personal information of EAC employees, contractors and the public.
- Identified and documented risks in EAC's operations for effectively identifying securing and protecting privacy data.
- Analyzed EAC's internal controls related to processes to safeguard privacy data, related policies and procedures, and records management.
- Tested significant controls to determine whether those controls are operating effectively to mitigate any identified risk.
- Issued Notice of Findings and Recommendations (NFRs) to EAC and discussed results with EAC and OIG.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Audit Findings and Recommendations

### **1. EAC had not implemented effective encryption mechanisms to appropriately protect agency information, including PII.**

We noted that EAC had not implemented effective encryption to appropriately protect agency information, including PII. Specifically, the following was noted:

- EAC did not employ encryption of all data stored on employee desktops or laptops. Additionally, we noted several instances where PII, including names, addresses, phone numbers and social security numbers, were located on the network and not password protected or encrypted.
- Backup tapes were not encrypted prior to being sent off-site.

We understand that EAC issued encrypted flash drives to staff, who are required to save sensitive or PII data on these flash drives before removal from the office. Also, EAC employees are required to utilize a designated encryption tool to store the data on their laptops.

Although all data stored on EAC laptops were not encrypted, we understand that all laptops are protected and monitored by a third party vendor responsible for monitoring the use of each laptop. In the event the laptop is lost or stolen, this vendor is capable of wiping the drive remotely as soon as they identify the computer online. EAC personnel could remotely access their shared drives via VPN and their email by means of a secured web site (SSL) using an Online Web Application.

EAC's Office of the Chief Information Officer (OCIO), backs up data using a password protected tool that requires using the same password to restore any data. In support of EAC's Disaster Recovery effort, PII data is encrypted by data owners prior to backing up the data to a tape drive and sending it to an offsite location for storage.

EAC management is presently developing a plan to upgrade workstations and laptops to an operating system platform, which has full-disk encryption capabilities. To address our recommendations, the OCIO and Privacy Officer have indicated they will perform a full scale review of the agency's shared drive to detect unprotected PII and ensure that files and folders are properly protected. At the same time, the SAOP will evaluate the backup device encryption capability of all backup tapes transported offsite for storage.

Section 1.2 of the *EAC Encryption Key Management* policy states, "all agency data on laptop and portable storage devices (e.g., USB flash drives, external hard drives) must be encrypted with a FIPS 140-2 certified encryption module." Additionally, section 1.3 states "if it is a business requirement to store PII on EAC user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, person digital assistants and Black berries, PII must be encrypted using a FIPS 140-2 certified encryption module."

National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, security control MP-5, states the following regarding media transport:



The organization:

- a. Protects and controls [Assignment: organization-defined types of digital and non-digital media] during transport outside of controlled areas using [Assignment: organization-defined security measures]; Control Enhancement:

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

EAC employees are encouraged by management to utilize the zipping tool, as an encryption mechanism for storing PII on laptops and other mobile devices; however, files must be stored on the EAC network prior to being compressed and encrypted. EAC is planning to move to the Windows 7 operating system which has built encryption. Additionally, the ability to encrypt backup tapes is available; however, it is a manual feature which EAC can turn on and off. The EAC encryption key was created during the audit period and use was unable to be verified. By not encrypting data, EAC is at an increased risk of data loss or theft.

### **Recommendations**

We recommend EAC management:

- 1) Develop and implement a plan to implement encryption to all data stored on agency laptops and workstations.
- 2) Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected.
- 3) Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.

### **2. Formalized PII usage reports were not submitted to the OIG in accordance with Section 522 of the Consolidated Appropriations Act of 2005.**

We noted that EAC management did not provide written PII usage reports to the OIG.

Section 522 of the *Consolidate Appropriations Act of 2005* states, "each agency shall prepare a written report of its use of information in an identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency. Each report shall be signed by the agency privacy officer to verify that the agency intends to comply with the procedures in the report. By signing the report the privacy officer also verifies that the agency is only using information in identifiable form as detailed in the report." (5 U.S.C. § 552a(c))

EAC completes the annual FISMA review which requires the agency to report on information privacy; although the FY 2012 FISMA audit and report did not address the agency's controls surrounding the protection of privacy data. Furthermore, management was unaware of the requirement to complete reports to provide to the OIG of their use and collection of PII, and their adherence of agency policy and regulations.

Without periodic reviews of agency use of PII, EAC may be unaware of the information that is being collected, used, and stored by the agency; therefore, the agency may inadvertently apply insufficient security controls to adequately protect that information.

#### **Recommendation**

We recommend EAC management 1) perform an inventory of EAC's PII data and how it is used within the agency and 2) document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.

### **3. *The EAC Records Management Processes and Procedures Standard Operating Procedure was not formally documented***

We noted that EAC had not finalized the Records Management Processes and Procedures Standard Operating Procedure as they were in the process of coordinating completion with National Archives and Records Administration (NARA). However, if procedures are not formally documented related to records management, documents may not be adequately encrypted or secured, additionally EAC is at an increased risk of data loss or theft of these records.

We understand that the draft of EAC's Records Management Processes and Procedures Standard Operating Procedures is currently being reviewed by the agency's Acting Executive Director and Chief Operating Officer, Senior Agency Official for Privacy, Privacy Officer, and outside counsel. Once comments have been agreed upon, they will be incorporated into the document and the SOP will be finalized.

Section 522 of Public Law 108-447 states as part of bullet (b)(1), "Within 12 months of enactment of this Act, each agency shall establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage and security of information in an identifiable form relating to the agency employees and the public. Such procedures shall be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act of 1974, and section 208 of the E-Government Act of 2002.

#### **Recommendation**

We recommend EAC finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

## Conclusions and Recommendations

Based upon our review, EAC has made improvements since the last Privacy audit to strengthen controls over the security of PII including conducting PIA, appointing a senior agency official for privacy and privacy officer, and developing formalized policies and procedures for PII, however more work remains to be accomplished. To become fully compliant with Section 522 of the Consolidated Appropriations Act 2005, EAC needs to ensure privacy role based training is performed, encryption controls to secure PII data stored on desktops, laptops and backup tapes are strengthened, and an ongoing review of and reporting to the OIG of PII usage within the agency and the finalization of records management policies. We recommend EAC management:

- Develop and implement a plan to apply data encryption to all agency laptops and workstations.
- Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected.
- Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.
- Perform an inventory of EAC's PII and how it is used within the agency.
- Document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.
- Finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

## Agency Response and OIG Comments

1. **EAC had not implemented effective encryption mechanism to appropriately protect agency information, including PII.**

### **Management Response**

Management initially disagreed with this finding related to the recommendation for full disk encryption, however also indicated the current use of encrypted flash drives and planned projects including operating system upgrades, data encryption implementation, review of all shared drives for unsecured PII and a reconfiguration project to mitigate the risks identified.

### **OIG Comments**

Revisions were made to the finding and recommendation within this report to address management's concerns related to full disk encryption. Management subsequently concurred with revised wording to data encryption.

2. **Formalized PII usage reports were not submitted to the OIG in accordance with Section 522 of the Consolidated Appropriations Act of 2005.**

### **Management Response**

Management agreed with the finding and recommendation and plans to conduct an inventory of EAC's PII and submit a PII usage report to the IG by the first week of July 2013.

### **OIG Comments**

Management concurred with our finding and recommendation.

3. **The EAC Records Management Processes and Procedures Standard Operating Procedure (SOP) was not formally documented.**

### **Management Response**

Management agreed with the finding and recommendation and indicated EAC's Records Management Standard Operating Processes and Procedures was signed and approved on April 4, 2013.

### **OIG Comments**

Management concurred with our finding and recommendation.



**U.S. ELECTION ASSISTANCE COMMISSION**  
1201 New York Avenue, NW, Suite 300  
Washington, DC 20005

Memorandum

April 9, 2013

To: Arnie Garza  
Assistant Inspector General for Audits

From: Alice Miller  
Acting Executive Director & Chief Operating Officer

Subject: 2012 Review of the U.S. Elections Assistance Commission  
Compliance with Section 522 of the Consolidated Appropriations  
Act 2005

This memorandum transmits the U.S. Election Assistance Commission's (EAC) responses to the recommendations resulting from the audit performed by CliftonLarsonAllen (CLA) between November 2012 and January 2013. As stated in the draft report, the purpose of the audit was to review EAC's compliance with Section 522 of the Consolidated Appropriations Act 2005.

We are pleased that CLA notes the proactive and significant progress that EAC's Privacy Act Program has made in addressing our statutory responsibilities. We consider privacy to be a matter of great importance and have undertaken significant efforts to ensure compliance.

This memorandum: (1) identifies management's agreement and disagreement with the recommendations; and (2) identifies actions that EAC will take to address the recommendations.

EAC's response to each CLA recommendation follows:

## **1. ENCRYPTION MECHANISMS**

**Recommendation:** Develop and implement a plan to apply full-disk encryption to agency laptops and workstations. Perform a review for unprotected PII stored on the network share drives to ensure files are adequately protected. Implement a validation process to ensure encryption of all backup tapes being transported off-site for storage.

**Management Response: We disagree.** To administer internal security controls to protect sensitive and PII data, EAC issued encrypted flash drives to staff. Sensitive and PII data must be encrypted and saved on the hard drives on the server and the flash drives by the information owner.

As indicated in the audit report, efforts are being made by management to safeguard PII data. Current projects include:

- Developing a plan to upgrade workstations and laptops to Windows 7 and utilizing an encryption software application for the partitioned full-disk encryption of EAC workstations and laptops. Sample testing is currently underway.
- Partitioning the disk, thereby, separating the operating system (OS) from the data section. Since the OS does not have to be encrypted, the section containing data will be encrypted on all EAC laptops and workstations.

The Senior Agency Officer of Privacy (SAOP) and the Privacy Officer (PO) will perform a full scale review of the agency's shared drive to ensure that files and folders are properly protected and security access permissions are updated. During this process, active and inactive files will be identified to facilitate the reconfiguration of the shared drive. Active files that can be viewed by all EAC staff will be placed in an Access Central folder; whereas, active files containing PII and sensitive data will be placed in Division folders and accessible via security access permissions. Inactive files will be archived, by division, and will also require security access permissions. To that end, the reconfiguration project will (1) provide increased space on the shared drive, (2) decrease the amount of time it takes to back up the t-drive, and (3) facilitate encryption of all backup tapes being transported off-site for storage.

## 2. PII USAGE REPORTS

**Recommendation: We agree.** Perform an inventory of EAC's PII data and how it is used within the agency and document and implement a process for the Privacy Officer to periodically report to the Office of Inspector General on the Agency's use of information in an identifiable form, and verify compliance with privacy and data protection policies and procedures.

**Management Response:** An inventory of EAC's PII and how it is used in the agency will take place during the current Records Management project, which is expected to be completed by the third quarter in FY 2013. The PO will submit a PII usage report to the IG by the first week in July.

## 3. RECORDS MANAGEMENT STANDARD OPERATING PROCEDURE (SOP)

**Recommendation:** Finalize and implement the Records Management Processes and Procedures Standard Operating Procedure.

**Management Response: We agree.** The final draft of EAC's Records Management Standard Operating Processes & Procedures was signed and approved by executive staff on April 4, 2013 and is currently on EAC's t-drive.

Thank you and the auditors for courtesies and assistance that was extended to our staff during the audit.

If you have any questions regarding our responses, please do not hesitate to contact me at (202) 566-3110.

Copy to: Mohammed Maeruf, CIO  
Annette Lafferty, CFO  
Sheila Banks, PO

## MANAGEMENT RESPONSES TO RECOMMENDATIONS

This table presents management’s responses to the recommendations in the draft audit report and the status of the recommendations as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Measure	Expected Completion Date	Responsible Party(ies)	Resolved:* Yes/ No	Open or Closed**
1	EAC workstations and laptops will be upgraded to Windows 7. IT is currently testing the several encryption software applications to support this task  Review, restructure, and update security access to agency’s shared drive.	Encryption of data contained on partitioned disk. Full-disk encryption is not necessary.	December 31, 2013	Office of Chief Information Officer  Privacy Officer	No	Open
2	PII inventory and usage information will be collected along with information for the Records Management project.	Annual PII Usage Reports submitted to the Office of Inspector General (OIG)	July 5, 2013	Records Management Officer  Privacy Officer	Yes	Open
3	Implement the Records Management Standard Operating Processes and Procedures	Finalized Records Management Standard Operating Procedure	April 3, 2013	Acting Executive Director, Inspector General, Chief Financial Officer, Chief Information Officer, Privacy Officer	Yes	Closed

---

\* Resolved – (1) Management concurs with the recommendation, and the planned corrective action is **consistent** with the recommendation.  
(2) Management does not concur with the recommendation, but planned alternative action is **acceptable** to the OIG.

\*\* Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.

---

## **OIG's Mission**

The OIG audit mission is to provide timely, high-quality professional products and services that are useful to OIG's clients. OIG seeks to provide value through its work, which is designed to enhance the economy, efficiency, and effectiveness in EAC operations so they work better and cost less in the context of today's declining resources. OIG also seeks to detect and prevent fraud, waste, abuse, and mismanagement in these programs and operations. Products and services include traditional financial and performance audits, contract and grant audits, information systems audits, and evaluations.

---

## **Obtaining Copies of OIG Reports**

Copies of OIG reports can be requested by e-mail.  
([eacoig@eac.gov](mailto:eacoig@eac.gov)).

Mail orders should be sent to:

U.S. Election Assistance Commission  
Office of Inspector General  
1201 New York Ave. NW - Suite 300  
Washington, DC 20005

To order by phone: Voice: (202) 566-3100  
Fax: (202) 566-0957

---

## **To Report Fraud, Waste and Abuse Involving the U.S. Election Assistance Commission or Help America Vote Act Funds**

By Mail: U.S. Election Assistance Commission  
Office of Inspector General  
1201 New York Ave. NW - Suite 300  
Washington, DC 20005

E-mail: [eacoig@eac.gov](mailto:eacoig@eac.gov)

OIG Hotline: 866-552-0004 (toll free)

FAX: 202-566-0957

---





# **Exhibit 20**



## 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](mailto: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