ADMINISTRATIVE COMMUNICATIONS SYSTEM
U.S. DEPARTMENT OF EDUCATION

DEPARTMENTAL DIRECTIVE

OM: 6-108 **Page 1 of 45 (09/06/2016)**

Distribution:
All Department of Education Employees

Signed by: Andrew Jackson
Assistant Secretary for Management

Privacy: Section 208 of the E-Government Act of 2002 Policy and Compliance

Table of Contents

This is a new Directive. For technical questions regarding this Directive, please contact the Privacy Safeguards Division at Privacysafeguards@ed.gov or via telephone at (202) 401-1269.

I. Purpose

This Directive establishes policy and procedures at the United States (U.S.) Department of Education (ED) for implementing the privacy provisions of Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch. 36). This provision requires ED to conduct reviews of how information collected about individuals in identifiable form is handled within ED and to post guidance for privacy policies on agency websites used by the public. ED establishes policies and procedures for ED officials, employees, and contractors whose positions involve (1) the collection, maintenance, or dissemination of information about individuals in identifiable form when developing or procuring information technology (IT) systems or projects, (2) the initiation, consistent with the Paperwork Reduction Act, of a new electronic collection of information in identifiable form for 10 or more persons, or (3) the implementation of guidance documents issued by the Office of Management and Budget (OMB) in connection with the above activities as well as with respect to the privacy policies and notices posted on websites used by ED to engage with the public. ED is committed to instituting policies that protect information in identifiable form while promoting transparency and openness in government.

II. Policy

It is ED's policy to comply with all requirements of Section 208 of the E-Government Act of 2002, and to ensure that all IT systems that collect, maintain, or disseminate information in an identifiable form about the general public will document that privacy issues have been identified and adequately addressed.

III. Authorization

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch. 36) (Dec. 17, 2002) available at http://www.whitehouse.gov/omb/memoranda_m03-22 (Attachment B).

OMB Memorandum 99-18 "Privacy Policies on Federal Web Sites" (June 2, 1999) available at http://www.whitehouse.gov/omb/memoranda_m99-18.

OMB Memorandum 03-22 "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (Sept. 26, 2003) available at http://www.whitehouse.gov/omb/memoranda_m03-22.

OMB Memorandum 10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" (June 25, 2010) available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf and Appendix 6 in this document.

OMB Memorandum 10-23, "Guidance for Agency Use of Third-Party Websites and Applications" (June 25, 2010) available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

The Privacy Act of 1974, as amended (Privacy Act) (5 U.S.C. § 552a) available at http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf.

IV. Applicability

This Directive applies to all ED employees and contractors who operate, use, maintain, or manage Federal IT systems and electronic collections on behalf of ED.

V. Definitions

A. **Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014, Pub. L. 113-283 (Dec. 18, 2014) (FISMA)**: Legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or manmade threats. FISMA originally was signed into law as Title III of the E- Government Act of 2002.

B. **Individual**: An individual is a U.S. Person, which includes citizens of the United States (U.S.), and aliens lawfully admitted for permanent residence, and Non-U.S. Persons, which is any person who is not a "U.S. Person." [1]

C. **Information in Identifiable Form**: Information in an information technology system or online collection (1) that directly identifies an individual (*e.g.*, name, address, social security number or other identifying number or code, telephone number, e-mail address, *etc.*) or (2) 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.)

D. **Information Technology (IT)**: IT is any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

[1] The Department will apply the Privacy Act to individuals consistent with applicable exceptions and exemptions therein and it does not have the legal authority to apply and is not applying subsections (g) and (i) of the Privacy Act to information about non-U.S. persons.

E. **Maintain**: Maintain means to keep, collect, use, or disseminate.

F. **Major information system**: An information system that requires special management attention because of its importance to an ED mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

G. **Personally Identifiable Information (PII)**: As defined in OMB Memorandum M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (May 22, 2007), this term refers to information that can be used to distinguish or trace an individual's identity, such as his or her name, Social Security number, biometric records, *etc.*, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, *etc.*

H. **Privacy Impact Assessment (PIA)**: The PIA analyzes how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining and disseminating information in an identifiable form in an electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. OMB guidance on PIA requirements is available at http://www.whitehouse.gov/omb/memoranda/m03-22.html.

NOTE: Additional requirements and OMB guidance should be consulted if ED uses third-party websites or applications or if ED relies on a contractor (or other non-Federal entity) to operate a third-party website or application to engage with the public on ED's behalf: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

I. **Privacy Notice:** A privacy notice provides a brief description of how ED's privacy policy will apply in a specific situation. Because the privacy notice should serve to notify individuals before they engage with ED, a privacy notice should be provided on the specific webpage or application where individuals have the opportunity to make PII available to ED.

J. **Privacy Policy:** A privacy policy refers to the single, centrally located statement that is posted at or linked to at ED's principal website; any known, major entry points to ED's websites; or on any webpage that collects substantial information in identifiable form. The privacy policy should be a consolidated explanation of ED's general privacy-related practices that pertain to its official website and other online activities.

K. **Privacy Threshold Analysis (PTA)**: The privacy threshold analysis identifies whether the system collects and maintains PII, and whether additional privacy compliance documentation, such as a PIA or system of records notice (SORN), is required. A SORN is a notice required to be published in the Federal Register under the Privacy Act, and is discussed in ED ACS Directive OM: 6-104. The PTA is an initial document completed at the beginning of the system lifecycle by a Principal Office seeking to implement a system, program or project.

L. **Third-Party Websites or Applications**: Web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a non-government entity. For example, these technologies are located on a ".com" or ".org" website or other location that is not part of an official government domain (*e.g.,* ".gov"). Third-party applications can also be embedded or incorporated on an agency's official website.

M. **Web measurement and customization technologies**: These technologies are used to remember a user's online interactions with a website or online application in order to conduct measurement and analysis of usage or to customize the user's experience. These technologies may either be "single-session technologies" or "multi-session technologies." Such technologies include software scripts commonly called "cookies."

1. Single-session technologies are technologies that remember a user's online interactions within a single session or visit. Any identifier correlated to a particular user is used only within that session, is not later reused, and is deleted immediately after the session ends.

2. In contrast, multi-session technologies are technologies that remember a user's online interactions through multiple sessions. This approach requires the use of a persistent identifier for each user, which lasts across multiple sessions or visits.

VI. Responsibilities

A **Assistant Secretary for Management (ASM)**

1. Under OMB M-05-08, ED must identify and designate a senior official at the Assistant Secretary level to be the Senior Agency Official for Privacy (SAOP). The Secretary has identified the ASM, Office of Management (OM), as the SAOP.

2. The SAOP has overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including ED's

full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act. The SAOP plays a central role in overseeing, coordinating, and facilitating ED's compliance efforts and ensuring ED's employees and contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing ED's handling of personal information. Finally, the SAOP has a central policy-making role in ED's agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues, including those relating to ED's collection, use, sharing, and disclosure of personal information. The SAOP shall provide overall management, oversight, and resources for compliance with Section 208 the E-Government Act of 2002.

3. When a Principal Operating Component (POC) within ED is evaluating whether to use third-party websites or applications, the POC must consult with the SAOP as early as possible in the planning stage and continue to consult with the SAOP through the implementation and post-implementation process. Any proposals to use multi-session web measurement and customization technologies when PII is collected (also called "Tier 3") will be reviewed and approved by the SAOP (and also will need to be reviewed and approved by the Chief Information Officer (CIO)) after the proposal has been reviewed and approved by the Chief Privacy Officer (CPO).

B **Chief Privacy Officer (CPO)**

1. The SAOP directs the CPO to:

   a. Manage on a day-to-day basis ED's implementation of information privacy protections, so as to ensure ED's full compliance with federal laws, regulations, and policies relating to information privacy, including the Privacy Act, Section 208 of the E-Government Act of 2002, the FISMA, and policy and guidance issued by the Executive Office of the President, including OMB requirements regarding agency privacy policies listed in OMB M-03-22, M-10-22, and M-10-23.

   b. Participate in all organization information privacy compliance activities.

   c. Participate in assessing the impact of the organization's use of technology on privacy and the protection of personal information.

2. The CPO is the reviewing official for PIAs, ensuring that they meet the requirements of Section 208 of the E-Government Act. The CPO will approve and sign the PIA documentation and ensure that it is made publicly available on ED's website at http://www2.ed.gov/notices/pia/index.html.

3. The CPO is responsible for ED's website privacy policy, including coordinating with the Office of Communications and Outreach (OCO) on issues relating to web privacy policy implementation, and with the CIO on issues about web measurement and customization technologies and for ensuring all privacy policies are in machine-readable formats. Any proposals to use multi-session web measurement and customization technologies when PII is collected (also called "Tier 3") must be reviewed and approved by the CPO, prior to review and approval by the SAOP and ultimately the CIO.

4. The CPO, with the CIO, will annually review and approve ED's use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance, and to justify ED's continued use.

C **Chief Information Officer (CIO)**

1. The CIO is responsible for information resources management, and ensures that ED's Information Assurance Security Program is developed, implemented, and managed. The CIO provides guidance to ensure that the security elements of Section 208 of the E-Government Act are implemented appropriately.

2. After the SAOP has reviewed and approved the web measurement and customization technologies being used in a manner subject to Tier 3, and the use of the technologies has gone through notice and comment procedures, the CIO must provide explicit written approval of their use. This approval must be documented in ED's online Privacy Policy. The CIO also has the responsibility to determine whether to exempt the use of the technology from the "notice and comment" requirement if the CIO determines that the notice and comment requirement is reasonably likely to result in serious public harm.

3. The CIO, with the CPO, will annually approve ED's use of web management and customization technologies to ensure compliance with all laws, regulations and OMB guidance, to justify ED's continued use.

4. The CIO and CPO will coordinate on website privacy policy issues, including implementation, as well as web measurement and customization technologies, to ensure all privacy policies are in machine-readable formats.

D **Senior Staff for Privacy Safeguards (SSPS), Privacy and Information Collection Clearance Division (PICCD), Office of the Chief Privacy Officer (OCPO), OM**

The SSPS shall:

1. Develop procedures, documents, and guidance required to implement Section 208 of the E-Government Act, including PIAs, reporting formats, Directives, reports, templates, and handbooks.

2. Provide technical assistance to system and program managers in developing PTAs and PIAs.

3. Ensure that the rules governing employee conduct, training, and implementation of Section 208 of the E-Government Act requirements are current and sufficient.

4. Coordinate the preparation of an annual report to OMB on Section 208 of the E-Government Act.

5. Consult with the Office of the General Counsel (OGC) on all legal matters related to implementation of the E-Government Act within ED.

6. Work with Office of the Chief Information Officer Information Assurance Services (OCIO IA) and Information System Owners (ISO) to ensure that privacy policies are posted on agency websites used by the public and that privacy policies and notices comply with applicable Federal requirements, including, but not limited to, that they are translated into a standardized machine-readable format.

7. If web measurement or customization technologies are being used, coordinate with the ISO, OCO, OCIO IA, and the Information Systems Security Officer (ISSO) of the POC requesting the usage, to assure compliance with OMB M-10-22 requirements and ensure that clear and conspicuous notice is provided on website privacy policy, in accordance with the requirements of Section VII. G. of this Directive. If use is Tier 3, the SSPS will review and approve proposals to use Tier 3 technologies and will assist the ISO in Notice and Comment, as described in Section VII. G. in this Directive.

8. Track Tier 3 usage for OMB reporting requirement purposes.

9. Verify annually that the continuing use of all web measurement and customization is in compliance with the requirements of OMB M-10-22, as described in Section VII. H., particularly, Tier 3, and have the results of the review posted to ED's Open Government Webpage with a mechanism for the public to provide feedback.

10. Develop procedures, documents, and guidance to help achieve compliance with OMB Memorandum 10-22 "Guidance for Online Use of

Web Measurement and Customization Technologies" (June 25, 2010) in ED's use of web measurement and customization technologies, including third-party web measurement and customization technologies.

11. Develop procedures, documents, and guidance to help ensure compliance with OMB Memorandum 10-23 "Guidance for Agency Use of Third-Party Websites and Applications" (June 25, 2010) in ED's use of third-party websites or applications.

12. Work with ISOs to ensure that privacy policies that comply with applicable Federal requirements are posted on their POC's websites that are used by the public, including, but not limited to, machine readable policies for P3P (Platform for Privacy Preferences).

13. Determine the circumstances where ED's web-based activities warrant additional consideration of privacy implications.

E **Information Systems Security Officers (ISSOs)**

ISSOs shall:

1. Ensure that all compliance documentation required for systems under their management is completed.

2. Work with the ISOs to complete the PIA.

3. Review, approve, and sign the PIA.

4. Ensure that all employees and contractors in their POC whose work provides them with access to information in identifiable form are aware of their responsibility for protecting information of the public, employee, and agency.

5. In accordance with the ED policy, ensure that all employees and contractors complete annual Privacy Safeguards training and as appropriate, complete job specific security and/or privacy training.

6. Provide ISOs with input regarding the security controls for the ISO's systems and websites.

7. Provide ISOs with input regarding website privacy policies.

8. If web measurement or customization technologies are being used for a system within the ISSO's POC, coordinate with the SSPS, ISO, OCO, and OCIO IA, to assure compliance with OMB M-10-22 requirements. ISSOs will ensure that clear and conspicuous notice is provided on website

privacy policy, in accordance with the requirements of Section VII. G. of this Directive.

9. Assist OCO and the SSPS with the annual verification that the continuing use of web measurement and customization is in compliance with the requirements of OMB M-10-22, as described in Section VII. H.

F **Information System Owners (ISO)**

ISOs are responsible for the overall procurement, development, integration, modification, operation, and maintenance of an information system. The ISO has the responsibilities listed below unless he/she in writing designates another individual, such as the program or project manager or the ISSO, to carry out any of these responsibilities.

The ISO will:

1. Prepare a PTA, when initiating a new electronic information collection at the beginning of the system lifecycle.

2. Prepare a PIA when required.

3. Ensure that PIAs associated with their programs or systems are complete and accurate.

4. Ensure that PIAs are completed in a timely and accurate manner.

5. If the system includes a public facing website, prepare a website privacy policy as discussed in Section VII. F. of this Directive.

6. Make appropriate updates and ensure continued compliance with stated web privacy policies.

7. Review PIAs whenever a system change creates new privacy risks and at least every two (2) years for systems or programs for which they are responsible and update as needed.

8. Review each project for which they are responsible and ensure compliance with the security and privacy requirements described in each PIA.

9. Work with SSPS and ISSOs to ensure that privacy policies and notices that comply with applicable Federal requirements are posted on POC websites and, as feasible, on third-party websites and applications that ED uses to engage the public, including, but not limited to, machine readable policies for the Platform for Privacy Preferences Project (P3P). If the ISO

is using web measurement or customization technologies, the ISO will coordinate with the SSPS, OCO, OCIO IA, and the ISSO of the POC requesting the usage, to ensure compliance with OMB M-10-22 requirements and to ensure that clear and conspicuous notice is provided on website privacy policy, in accordance with the requirements of Section VII. G. of this Directive. The ISO will also annually verify that the continuing use of web measurement and customization is in compliance with the requirements of OMB M-10-22.

G **Office of Communications and Outreach (OCO)**

If an ISO is using web measurement or customization technologies, OCO will coordinate with the ISO, SSPS, OCIO IA, and the ISSO of the POC requesting the usage, to assure compliance with OMB M-10-22 requirements and ensure that clear and conspicuous notice is provided on website privacy policy, in accordance with the requirements of Section VII. G. of this Directive. OCO is responsible for tracking Tier 2 usage for OMB reporting requirement purposes. OCO will also verify annually that the continuing use of Tier 2 web measurement and customization is in compliance with the requirements of OMB M-10-22, as described in Section VII. H. Additionally, OCO manages, operates, and develops content policies and procedures for ED.gov, and manages web content on ED webpages. OCO works with SSPS to develop and publish privacy policies and notices on ED.gov websites, compliant with OMB M-10-23.

H Office of the Chief Information officer, Information Assurance (OCIO IA)

If web measurement or customization technologies are being used, OCIO IA will coordinate with the SSPS, the ISO, OCO, and ISSO of the POC requesting the usage, to assure compliance with OMB M-10-22 requirements and to ensure that clear and conspicuous notice is provided on website privacy policy, in accordance with the requirements of Section VII. G. of this Directive. If use is Tier 3, OCIO IA will review and approve proposals to use Tier 3 technologies, as described in Section VII. G. in this Directive. OCIO IA will also assist in verifying annually that the continuing use of web measurement and customization is in compliance with the requirements of OMB M-10-22, as described in Section VII. H.

I **General Counsel** (GC)

The GC is responsible for interpreting and advising on all legal matters related to the implementation of Section 208 of the E-Government Act and its implementing guidance requirements.

J Contractors

Contractors and their employees who develop IT systems or projects for ED that collect, maintain, or disseminate information in identifiable form from or about members of the public or who design, develop, or maintain an electronic system on behalf of ED in order to perform an agency function that collects information in identifiable form for 10 or more members of the public, shall work with the relevant POC's ISSO to ensure that the system complies with Section 208 of the E-Government Act and applicable OMB guidance. This may include drafting, with the assistance and approval of the SSPS, a PIA, and a website Privacy Notice.

VII. Procedures and Requirements

A. General Requirements of Section 208 of the E-Government Act

ED must:

1. Conduct PIAs for electronic IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public or who design, develop, or maintain an electronic system on behalf of ED in order to perform an ED function that collects information in identifiable form for 10 or more members of the public, and, in general, make the PIAs publicly available.

2. Monitor ED's systems and practices to determine when and how PIAs should be updated.

3. Update PIAs when a system change creates new privacy risks.

4. Post privacy policies on ED websites used by the public. A website privacy policy must be placed at ED's principal website as well as any known, major entry points to that site, and any webpage that collects substantial information in identifiable form.

   NOTE: Pursuant to subsequent OMB guidance, ED's privacy policy must describe ED's use of any third-party websites and applications and any web measurement and customization technologies. ED also must post privacy notices on the specific webpages or applications where individuals have the opportunity to make PII available to ED, and ED should, when feasible, provide links to the relevant privacy policies of the third-party websites and applications being used by ED.

5. Translate privacy policies into a standardized machine-readable format (a statement about site privacy practices written in a standard computer

language (not English text) that can be read automatically by a web browser.

6. Report annually to OMB on compliance with Section 208 of the E-Government Act of 2002. *See* Office of Management and Budget Memorandum M-03-22 OMB "*Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*" (September 26, 2003).

B. **Privacy Threshold Analysis (PTA)**

POCs must conduct a PTA for all proposed systems to determine if, and to what extent, the system collects, maintains, or disseminates information in identifiable form, and whether additional privacy compliance documents are required. For a template, see Appendix 2.

C. **Privacy Impact Assessment (PIA)**

1. Section 208 of the E-Government Act mandates that agencies complete PIAs to ensure sufficient protections for the privacy of information in identifiable form as agencies implement citizen-centered electronic government. The PIA process requires ED to review the handling of information in identifiable form that is collected electronically from 10 or more persons or that is collected, maintained, or disseminated through the developing or purchasing new IT systems. For a template, see Appendix 4.

2. PIAs are intended to provide ED with the tools to make informed policy, system design or procurement decisions based on: an understanding of privacy risk and the options for mitigating that risk; ensuring that system and program managers are accountable for the proper handling of privacy issues; establishing a consistent format and structured process for analyzing both technical compliance and legal sufficiency with applicable privacy laws and regulations, as well as accepted privacy policy; providing basic documentation on the flow of personal information within ED systems for use and review by policy, program and management staff, systems analysts, and security specialists; and providing the public with assurances that their personal information is adequately protected by ED.

3. In conducting a PIA, SSPS must ensure that:

   a. changes in technology or business practices that are identified during the PIA process are evaluated,

   b. ISOs, SSPS, and appropriate IT experts participate in conducting the PIA, and

c. the quality and thoroughness of each PIA is assessed, and reviews are conducted to ensure that appropriate standards for PIAs are maintained.

4. When to conduct a PIA:

   a. A Principal Office must complete a PIA before it develops or procures an IT system or embarks on a new project that collects, maintains, or disseminates information in identifiable form, from or about members of the public or before conducting a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).

   b. PIAs must be reviewed whenever a system change creates new privacy risks and at least every two (2) years, and updated if a system change creates new privacy risks or to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form. For examples of system changes that create new privacy risks, see Appendix 3.

5. Circumstances in which a PIA is not required:

   a. A PIA is not required when an existing umbrella PIA adequately covers a new system, website or application, *e.g.*, Social Media Websites and Applications.

   b. A PIA is not required where the individually identifiable information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy risks are unchanged. For examples of situations where privacy risks are unchanged, see Appendix 3.

D. **PTA and PIA Procedures**

1. The ISO or designee will complete a PTA and submit it to the SSPS, who will then determine whether additional privacy documents must be completed.

2. If the PTA shows that a PIA is not necessary, the SSPS notifies the ISO that no further action is needed and the PTA is retained with the system documents.

3. If the PTA shows that a PIA is necessary, the SSPS notifies the ISO that a PIA must be completed.

4. The ISO will complete the PIA with the assistance of the Principal Office's ISSO, and the SSPS. For template, see Appendix 4. For a sample PIA, see Appendix 5, or go to ED's list of PIAs at http://www2.ed.gov/notices/pia/index.html

5. The ISO submits the PIA to SSPS for review and comment.

6. Once the PIA is in final, the ISO will obtain the appropriate signatures, and resubmit it to the SSPS for final approval.

7. The CPO will review, approve, and sign the PIA.

8. Once the CPO has signed the PIA, it will be posted to the ED's website at http://www2.ed.gov/notices/pia/index.html. The Principal Offices may post duplicate PIAs on their respective websites after the official one has been posted to ED's primary website. The official PIA is the one posted at ED's primary website.

9. When undertaking a new electronic information collection, the PIA shall be conducted and may be submitted to OMB, as part of the OMB 83-I Supporting Statement (the request to OMB to approve a new agency information collection) and made publicly available, unless an exception applies. An exception would apply when 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.

10. When a system is inactive, the SSPS may remove the PIA from an agency website after consulting with the Principal Office, OGC, OCPO.

11. See Appendix 1 for flow chart of detailed procedures.

E. **PIA for Third-Party Websites or Applications**

1. ED requires an adapted PIA when ED uses third-party websites or applications that make PII available to ED.

2. Each adapted PIA should be tailored to address the specific functions of the website or application. Once approved, the PIA is required to be posted on ED's official website as discussed above.

3. Many of ED's third-party website and application uses are covered under an existing umbrella PIA, titled Social Media Websites - Privacy Impact Assessment. If the SSPS determines that the new use of a third-party website or application is: a) functionally comparable with the uses listed in

this umbrella PIA; b) involves substantially similar practices; and c) does not raise distinct privacy risks, a new PIA may not need to be drafted. A link to that site must be placed on OCO's social media list found at http://www2.ed.gov/about/overview/focus/social-media.html. To be listed on that page, contact the Web Services team in OCO. If the site is not a social media website or application, a separate link will be placed at http://www2.ed.gov/notices/pia/index.html.

4. An adapted PIA should describe:

   a. The specific purpose of the ED's use of the third-party website or application;

   b. Any PII that is likely to become available to ED through public use of the third-party website or application;

   c. ED's intended or expected use of PII;

   d. Whether ED will share PII and, if so, with whom;

   e. Whether and how ED will maintain PII, and for how long;

   f. How ED will secure PII that it uses or maintains;

   g. What other privacy risks exist and how ED will mitigate those risks; and

   h. Whether ED's activities will create or modify a "system of records" under the Privacy Act in accordance with OMB Memorandum M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" (June 25, 2010).

F. **Website Privacy Policies**

1. ED's websites, known major entry points to ED's sites, and any webpage that collects substantial information in identifiable form must include a privacy policy.

2. The SSPS must determine the circumstances where ED's web-based activities warrant additional consideration of privacy implications.

3. The ISO must make appropriate updates and ensure continued compliance with stated web privacy policies.

4. The CIO must ensure the machine-readability of public-facing organization websites (*i.e.*, use of P3P).

5. Each policy must clearly and concisely inform visitors to the site what information ED collects about individuals, why ED collects it, and how ED will use this information.

6. Website privacy policies must be clearly labeled and easily accessed.

7. Website privacy policies must be translated into machine-readable formats that alert users automatically about whether the website's privacy practices match their personal privacy preferences.

8. Website privacy policies also must address "consent" to the collection and sharing of information about visitors. As such, ED must ensure that its privacy policies: a) inform visitors whenever providing requested information is voluntary; b) inform visitors how to grant consent for use of voluntarily-provided information; and c) 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.

9. Website privacy policies also must address any rights that website visitors have under the Privacy Act or other privacy laws. ED must notify website visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (including the Family Educational Rights and Privacy Act, as amended, enacted as section 444 of the General Education Provisions Act) in the body of the web privacy policy; *via* a link to the applicable agency regulation (*e.g.,* Privacy Act regulation and pertinent SORN); or *via* a link to another official summary of statutory rights.

10. When ED collects information subject to the Privacy Act, ED must explain that the information is maintained in a Privacy Act system of records and provide a Privacy Act Statement, as described in ACS Directive OM:6-107 at the point of collection. 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, the effects of not providing all or any part of the requested information, and the routine uses for which the requested information may be disclosed. (Note: Privacy Act Statements must contain additional information if the individual's Social Security number is requested).

11. Website privacy policies also must address the security of any Privacy Act-protected information collected *via* the website. In clear language, websites need to provide information about management, operational, and technical controls ensuring the security and confidentiality of the records (*e.g.,* access controls, data storage procedures, periodic testing of safeguards, *etc.*), and provide general 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.)

12. Additionally, if ED uses third-party websites or applications to collect PII, ED's website privacy policy must include:

    a. The specific purpose of ED's use of the third-party websites or applications;

    b. How ED will use PII that becomes available through the use of the third-party websites or applications;

    c. Who at ED will have access to PII;

    d. With whom PII will be shared (outside of ED);

    e. Whether and how ED will maintain PII, and for how long;

    f. How ED will secure PII that it uses or maintains; and

    g. What other privacy risks exist and how ED will mitigate those risks.

13. In addition to the above requirements, if ED uses third-party websites or applications to collect PII, to the extent feasible, ED should post a Privacy Notice, as described in OMB Memorandum 10-23 "Guidance for Agency Use of Third-Party Websites and Applications" (June 25, 2010) on the third-party website or application.

14. If ED uses web measurement and customization technologies itself or uses third-party web measurement and customization technologies on ED's behalf, OMB requires that ED's website privacy policy contain the following elements as set forth in Attachment 3 to OMB Memorandum 10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" (June 25, 2010):

    a. The purpose of the web measurement and/or customization technology;

    b. The usage tier, session type, and technology used;

    c. The nature of the information collected;

    d. The purpose and use of the information;

    e. Whether and to whom the information will be disclosed;

f. The privacy safeguards applied to the information. Cite whether or not a PIA or SORN is associated with the Website;

g. The data retention policy for the information;

h. Whether the technology is enabled by default or not and why;

i. How to opt out of the web measurement and/or customization technology; it is essential that this process be transparent and easy to follow;

j. A statement that opting out still permits users to access comparable information or services;

k. The identities of all third-party vendors involved in the measurement and customization process; and

l. If Tier 3 technologies are employed and the CIO does not exempt the technology from the notice and comment requirement, the policy must refer to the fact that public notice and comments were sought. Also note that both the SAOP and CIO provided written approval for the use of Tier 3 technologies on the website.

G. Online Use of Web Measurement and Customization Technologies:

1. During the usual compliance documentation process, a PTA identifies systems/websites that plan to use web measurement and customization technologies.

2. If use is Tier 1 - single-session - the ISO, the SSPS and OCO will coordinate to assure compliance with OMB M-10-22 requirements and ensure that clear and conspicuous notice is provided on website privacy policy.

3. If use is Tier 2 – multi-session without PII - the ISO, the SSPS, OCO, OCIO IA, and the ISSO of the POC requesting the usage, will coordinate to ensure that the POC is in compliance with OMB M-10-22, including “opt-out” options, that there is clear and conspicuous notice on the website’s privacy policy, and that the technology is being implemented appropriately. OCO will track Tier 2 usage for OMB reporting requirement purposes.

4. If use is Tier 3 – multi-session with PII:

a. The ISO must obtain the following approvals prior to deploying the technologies on an ED public-facing website.

b. The proposed use must be reviewed and approved by OCO, OCIO IA, the SSPS, and the ISSO of the POC requesting the usage. It is then referred to the CPO.

c. The CPO must review and approve the proposal to use Tier 3 technologies.

d. The SAOP next must review and approve the proposal to use Tier 3 technologies.

e. After the SAOP's review and approval, for new proposals for Tier 3 uses, or substantive changes to existing uses of such technologies, ED must:

1) Unless waived by the CIO, solicit comment through the ED Open Government Webpage for a minimum of 30 days, as described in OMB M-10-22.

2) Review and consider substantive comments and make changes to the intended use of the technologies where appropriate.

3) Notice and Comment can only be waived with written approval from the CIO if the process is reasonably likely to result in serious public harm.

4) After the Notice and Comment process, the CIO must provide explicit written approval to use Tier 3 technologies. The CIO's and SAOP's approval must be cited in ED's Privacy Policy.

5) The SSPS will track Tier 3 usage for OMB reporting requirement purposes.

H. **Verification of Compliance**

1. ED must annually review its use of web measurement and customization technology to verify that such use is in compliance with the requirements of OMB M-10-22.

2. Results of the review will be posted on ED's Open Government webpage with a mechanism for the public to provide feedback.

3. Verification will be performed as follows:

a. Tier 1 – OCO and the ISOs will lead the review, with assistance from SSPS, OCIO IA, and the ISSO from the POC where the technology is being used.

b. Tier 2 – OCO and the ISOs will lead the review with assistance from SSPS, OCIO IA, and the ISSO from the POC where the technology is being used.

c. Tier 3 – the SSPS will lead the review with assistance from OCO, the ISO, OCIO IA, and the ISSO from the POC where the technology is being used.

I. E-Government Act Reporting Requirements

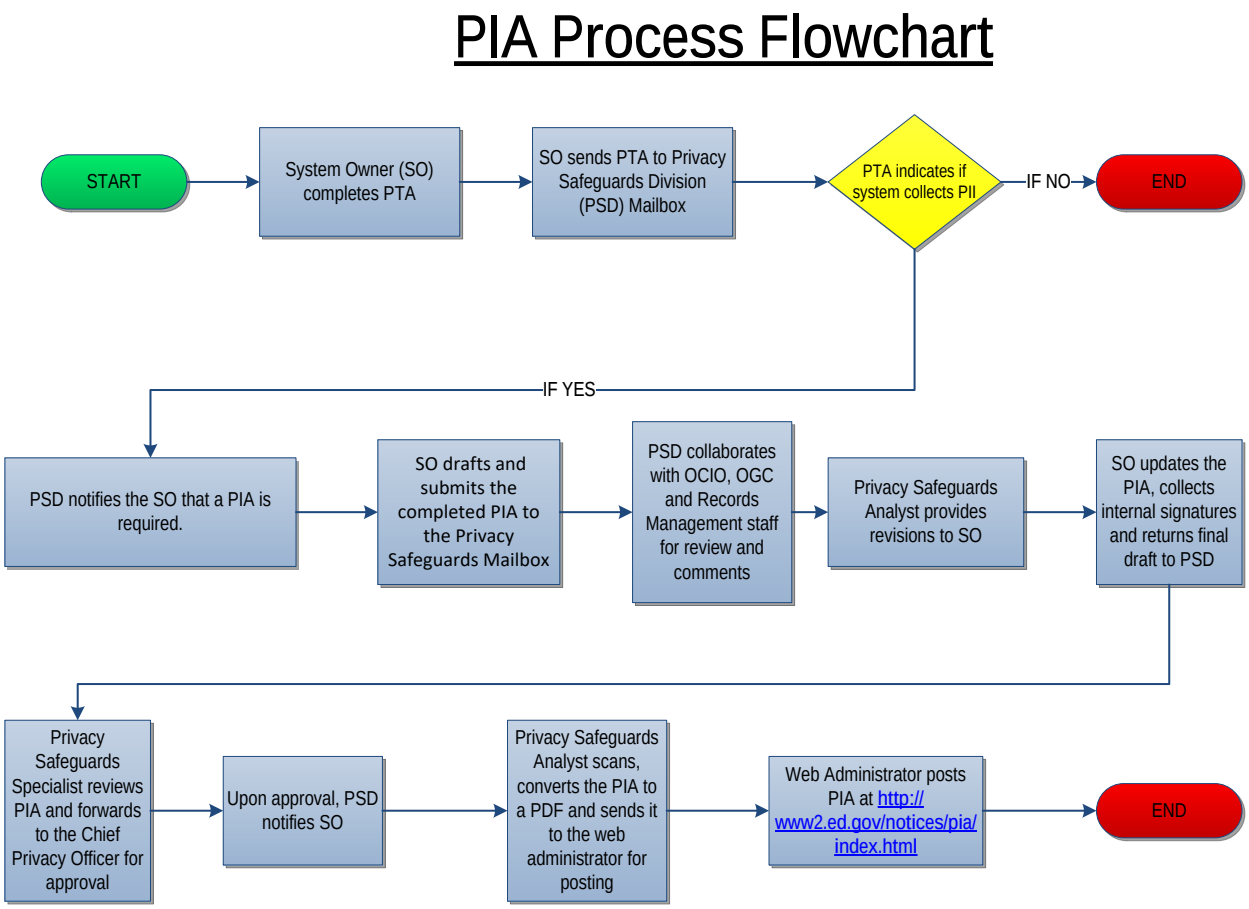
Each year, the CPO will prepare for the SAOP a report of ED activities as part of ED's annual E-Government Act status report submitted to OMB. This report must address the following three (3) elements for IT systems or information collections for which PIAs were conducted:

1. Include the mechanism by which the PIA was made publicly available (if made available in summary form or not at all, explain). If made available in conjunction with an Information Collection Request (ICR) or SORN, include the publication date of the PIA.

2. Agency achievement of goals for machine readability. Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.

3. Contact information. Include the individual(s) (name and title) appointed by the head of the agency to serve as the agency's principal contact(s) for IT/Web matters and the individual (name and title) primarily responsible for privacy policies.

Appendix 1: Privacy Impact Assessment Flow Chart



Appendix 2: Privacy Threshold Analysis Template

DEPARTMENT OF EDUCATION (ED)

PRIVACY THRESHOLD ANALYSIS (PTA)

Pursuant to Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36), a Privacy Impact Assessment (PIA) is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed electronically by a federal agency. Personally Identifiable Information (PII) (also known as information in identifiable form ("IIF")) is information that directly or indirectly identifies an individual, and is defined in more detail below. Federal law and regulations require that, under certain circumstances, a federal agency perform and make available to the public a PIA to analyze how privacy issues were considered when developing a new Information Technology (IT) system or initiating a new electronic information collection, or when a system change creates new privacy risks.

In order to minimize the potential burden of the PIA process on system owners and managers, ED's Privacy Safeguards Division has developed a Privacy Threshold Analysis (PTA) form that provides an efficient manner to determine if a system requires a PIA.

Instructions: Complete a PTA for each system(s) for which you are responsible and return it by E-mail to ED's

Privacy Safeguards Division at: E-mail: privacysafeguards@ed.gov

If you have any questions or need assistance with completing the PTA, contact ED's Privacy Safeguard

Division by E-mail at privacysafeguards@ed.gov or call the service line at 202-401-1269.

The Privacy Safeguards Division will inform you if a PIA is required. The PIA form is available on the Privacy

Safeguards webpage at: https://connected.ed.gov/om/Pages/Privacy-Safeguards-Division.aspx

Date:

Name of Program/System:

ED Principal Office:

Program Manager or System Owner Name:

Title/Role

Phone and E-mail

1. Provide a general description of the system and its purpose.

2. Does the system collect, maintain, or disseminate PII about individuals - either internal (ED employees and/or contractors) or external ED community (parents, teachers, general public, *etc.*)?

☐ Yes or ☐ No. If yes, proceed to question 3. If the answer is No, the assessment is complete – send to the Privacy Safeguards Program Office.

3. Please identify the type of PII that would be collected or used such as name, SSN, date of birth, place of birth, home address, home phone, personal email, medical information, financial information, educational information, biometrics, *etc.*

4. Has this system been previously assessed under an evaluation similar to a PIA?
☐ Yes or ☐ No. If the answer is yes, describe the evaluation.

5. Status of System: (Select from drop down box)

6. Has a system change occurred that creates new privacy risks (paper to electronic system, new use or disclosure of data, merging databases, new public access, *etc.*)?
☐ Yes or ☐ No. If the answer is yes, please describe the system change.

7. Is the system a major application? (A "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.) ☐ Yes or ☐ No

Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

8. Does your program or system plan to use a third party website or application

(*e.g.,* Facebook, Twitter, *etc.*), or have you hired a contractor to operate a website or application to engage with the public on ED's behalf?

9. Does your program or system plan to use web measurement and customization technologies (*e.g.*, cookies, web analytics, or any other technology that remembers a user's online interaction) on a website that engages with the public?

10. Is there a Certification and Accreditation record within the FISMA tracking system?
☐ Yes or ☐ No. If the answer is yes, please include the date.

Appendix 3: When to Conduct a PIA

Examples of System Changes that Require Updates to PIAs due to New Privacy Risks

1. Conversions – when converting from paper-based records to electronic systems;

2. Anonymous to non-anonymous – when functions applied to an existing information collection change anonymous information into information in identifiable form;

3. Significant system management changes – when new uses of existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;

4. 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;

5. New public access – when user-authenticating technology (*e.g.,* password, digital certificates, biometric) is newly applied to an electronic information system accessed by members of the public;

6. 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 requirements);

7. 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;

8. 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; or

9. Alterations in the character of the data – when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health and financial information).

Examples of situations where privacy risks are unchanged and a PIA is not required:

1. 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);

2. 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;

3. 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);

4. 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;

5. 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;

6. 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; or

7. For minor changes to a system or collection that do not create new privacy risks.

Appendix 4: Privacy Impact Assessment Template

NOTE: this PIA template should not be used to analyze third-party websites or applications. Please see the Privacy Safeguards Team for the appropriate Template for a modified PIA.

Privacy Impact Assessment

For:

Date:

Point of Contact:

Information System Owner (ISO):

Author:

Office of [Principal Office Name Here]

U.S. Department of Education

1. **System Information**. Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

2. **Legal Authority**. Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

3. **Characterization of the Information**. What elements of personally identifiable information (PII) are collected and maintained by the system (*e.g*., name, Social Security number, date of birth, address, phone number)? Who is or what are the sources of the information (*e.g.,* student, teacher, employee, school, university)? How the information is collected (website, paper form, on-line "contact us" form)? Is the information used to link or cross-reference multiple databases?

4. **Purpose of Information Collected**. How is this information necessary to accomplish the mission of the program or to contribute to a necessary agency activity? Is the data collected only that which is necessary to accomplish the legitimate business purpose? Given the amount and any type of data collected, discuss the privacy risks identified and how they were mitigated.

5. **Social Security Numbers (SSNs).** If SSNs are collected and used, describe the purpose of the collection, the type of use, and any intended disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If the system collects SSNs, the PIA will require a signature by your POC's Assistant Secretary or designee.

6. **Uses of the Information.** How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Does the system also use commercial information, publicly available information, or information from other Federal agency databases?

7. **Internal Sharing and Disclosure.** With which internal ED offices/programs will the information be shared? What information is shared? For what purpose is the information shared?

8. **External Sharing and Disclosure.** With what external entities will the information be shared (*e.g.,* another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of ED? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding, or other type of approved sharing agreement with another agency?

9. **Notice.** Is notice provided to the individual prior to collection of his or her information (*e.g.,* a posted Privacy Notice or a Privacy Act Statement)? What opportunities do individuals have to decline to provide information (where providing

the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how do individuals grant consent?

10. **Web Addresses.** List the web addresses (known or planned) where a Privacy Notice will be posted.

11. **Security.** What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a Security Authorization been completed? Is the system compliant with federal security requirements?

12. **Privacy Act System of Records.** Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is there an ED or Federal Government-wide system of records notice (SORN)? If a SORN already exists, what is the SORN Name and Number?

13. **Records Retention and Disposition.** Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes, provide the records schedule number.

Certifying Officials' Signatures:

Senior Program Official **Date**

Information System Owner/Information System Security Officer **Date**

FOR SYSTEMS THAT COLLECT, MAINTAIN AND/OR TRANSFER SSNS

Assistant Secretary for Principal Operating Component or designee Date

Kathleen Styles, Chief Privacy Officer **Date**

Appendix 5: Sample Privacy Impact Assessment

Privacy Impact Assessment

For

Federal Student Aid Information Center (FSAIC)

Date:

10/16/2016

Point of Contact:

Shital M. Shah
Shital.Shah@ed.gov
(202) 377-4028

System Owner:

Diana O'Hara
Diana.OHara@ed.gov
(202) 377-3466

Author:

Shital M. Shah
FSAIC Information System Security Officer (ISSO)

Office of Federal Student Aid
U.S. Department of Education

1. **System Information**. Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

   Federal Student Aid (FSA) Federal Student Aid Information Center (FSAIC) system is a government call/contact center that performs all customer service functions associated with receiving and responding to potential and current Free Application for Federal Student Aid (FAFSA) applicants such as students, parents, as well as counselors, schools, and other public inquirers (herein collectively referred to as FSAIC customers) with questions on a wide range of topics throughout the entire financial aid process, including preparing for college, the types of student aid, aid eligibility, applying for aid, and managing student loans through the use of various communications media, including telephones, telecommunication devices for the deaf (TDD/TTY), email, fax, postal mail, web chat, social media, and other media as appropriate.

2. **Legal Authority**. Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

   The Higher Education Act of 1965 (Public Law 89–329), as amended, sections 428, 484, and 485B; 31 United States Code (U.S.C). 7701; and Executive Order 9397 (November 22, 1943), as amended by Executive Order 13478 (November 18, 2008).

3. **Characterization of the Information.** What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

   FSAIC system collects and maintains following elements of personally identifiable information (PII). The sources of PII are Students (and his/her spouse, if applicable) and parental information for dependent students as well as counselors, schools, and other public inquirers. The PII collected is either through on-line (Customer Relationship Management (CRM), phone (audio) and video (desktop) recordings, and/or in paper-form (fax and/or postal mail Control Correspondence)). The FSAIC customer PII collected could be any of the following elements or a combination thereof :

   a. Social Security number (SSN),

   b. Name (first, last and middle initial),

   c. Date of Birth (DOB),

d. Street Address,

e. Telephone number,

f. Email Address,

g. Driver license number and state of issuance,

h. Citizenship status,

i. Marital status (including month and year of marriage),

j. State of legal residence, date of legal residency, if applicable,

k. Sex/Gender,

l. Education level.

The FSAIC customers' PII is not linked or cross referenced with any databases.

4. **Why is the information collected**? How is this information necessary to the mission of the program, or contributes to a necessary agency activity? Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

   FSAIC system collects and maintains PII to:

   a. Assist FSAIC Customer Service Representatives (CSRs) in properly documenting the interaction with FSAIC customers and to provide the necessary contact information so that CSRs can perform follow up activities with the customer.

   b. Implement CSRs quality monitoring process so that the quality team can monitor and provide feedback and training to the CSRs on their interactions with FSAIC customers.

   c. Verify the identity of the customer as well as to access the FSAIC customers' information in other FSA applications such as Person Authentication Service (PAS), Central Processing System (CPS), and National Student Loan Database System (NSLDS)

   Privacy risks are mitigated by encrypting and/or masking the customers' PII and/or by controlling access to the customer information on a need to know basis as well as by requiring two-factor authentication. Additionally, devices on which the customers PII are stored are maintained in secured server rooms with limited physical access to authorized personnel only. Intrusion Prevention Systems (IPS) and Firewall devices are also in place to protect access to this information. All FSAIC personnel

are also required to obtain a public trust security clearance, sign the FSAIC Rules of Behavior document, and to complete security awareness training on an annual basis.

5, **Social Security Number (SSN).** If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

   FSAIC has considered alternatives to the collection of Social Security Number (SSN). However, SSN being a unique identifier for Title IV programs, its collection and use is required to verify the identity of the FSAIC customer as well as to access the FSAIC customers' information in other FSA applications such as PAS, CPS, and NSLDS and assist FSAIC customers with their questions on a wide range of topics throughout the entire financial aid process.

6. **Uses of the Information.** What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

   FSAIC system collects, maintains, and uses FSAIC Customers' PII to;

   a. Assist FSAIC Customer Service Representatives (CSRs) in properly documenting the interaction with FSAIC customers and to provide the necessary contact information so that CSRs can perform follow up activities with the customer.

   b. Implement CSRs quality monitoring process so that the quality team can monitor and provide feedback and training to the CSRs on their interactions with FSAIC customers.

   c. Verify the identity of the FSAIC customer as well as to access FSAIC customers' information (including the loan information as per the Higher Education Act of 1965 (Public Law 89–329), as amended) in other FSA applications such as PAS, CPS, and NSLDS.

7. **Internal Sharing and Disclosure.** With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

   Control correspondence information captured via the CRM application is only accessible by authorized FSA and contractor personnel to respond to control correspondence inquiries from FSAIC customers. The information captured

during the desktop and audio recording process is shared with FSA personnel who assist in the monitoring and training of FSAIC CSRs.

8. **External Sharing and Disclosure.** With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

   The information captured and maintained by FSAIC system is not shared with any external entities outside of FSA**.**

9. **Notice.** Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

   The CRM on-line application contains a detailed Privacy Act notice. The customer data referred to during FSAIC customer service calls originates from the Free Application for Federal Student Aid (FAFSA); the FAFSA website (www.studentaid.ed.gov) contains a detailed Privacy Act notice. Additionally, the prompt within the FSAIC telephony/Integrated Voice Response (IVR) system discloses to the customers that their calls may be recorded for quality purposes.

10. **Web Addresses. List the web addresses (known or planned) that have a Privacy Notice.**

    The following sub-bullets (a and b) are the two FSAIC web addresses and the privacy notices for those web addresses is located at https://studentaid.ed.gov/sa/privacy.

    a. https://studentaidhelp.ed.gov

    b. https://studentaidhelp-es.ed.gov/app/home

11. **Security.** What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

    In accordance with the Federal Information Security Management Act of 2002 (FISMA) and the Federal Information Security Modernization Act of 2014, every FSA system must receive a signed Authority to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security

controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program. FSAIC received its ATO on 09/18/2015.

FISMA controls implemented comprise a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

12. **Privacy Act System of Records**. Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

    The FSAIC will be included in Federal Student Aid Application File System of Records Notice, (SORN) # 18-11-01 (76 FR 149 46774-81).

13. **Records Retention and Disposition**. Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

    The records disposition schedule is ED 072: FSA Application, Origination, and Disbursement

    Files Disposition: Temporary. Destroy/Delete 15 years after final repayment or audit of student financial obligation, or after student record information is transferred to alternate recordkeeping system (i.e., loan servicing system), whichever is sooner.

    The National Archives and Records Administration (NARA) Disposition Authority is N1-441-09-23.

    FSAIC has a procedure in place for the storage and retention of documents received via postal mail/correspondence. This procedure states that the agent attaches a PDF of the postal correspondence to the incident record within the CRM application. Data, including incident tickets and uploaded PDFs of documents received via postal correspondence, are maintained in the CRM application for the life of the contract.

Appendix 6: OMB M-10-22

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

June 25, 2010

M-10-22

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Peter R. Orszag
Director

SUBJECT: Guidance for Online Use of Web Measurement and Customization Technologies

On January 21, 2009, the President issued a memorandum calling for the establishment of "a system of transparency, public participation, and collaboration."[1] The memorandum required an *Open Government Directive* to be issued by the Director of the Office of Management and Budget (OMB), instructing "executive departments and agencies to take specific actions implementing the principles set forth in this memorandum." Implementing the President's memorandum, OMB's *Open Government Directive* requires a series of measures to promote the commitments to transparency, participation, and collaboration.[2]

As the Internet continues to evolve, the Federal Government has new opportunities to promote these commitments by engaging with citizens, explaining what Federal agencies are doing, seeking public comments, and improving the delivery of services. In the private sector, it has become standard for commercial websites to use web measurement and customization technologies to engage with members of the public.

For government agencies, the potential benefits of web measurement and customization technologies are clear. With the help of such technologies, agencies will be able to allow users to customize their settings, avoid filling out duplicative information, and navigate websites more quickly and in a way that serves their interests and needs. These technologies will also allow agencies to see what is useful to the public and respond accordingly. Services to customers and users can be significantly improved as a result.

---

[1] President Barack Obama, Memorandum on Transparency and Open Government (Jan. 21, 2009), *available at* http://www.gpoaccess.gov/presdocs/2009/DCPD200900010.pdf

[2] OMB Memorandum M-10-06, *Open Government Directive* (Dec. 8, 2009), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf

At the same time, OMB is acutely aware of, and sensitive to, the unique privacy questions raised by government uses of such technologies. Any such uses must not compromise or invade personal privacy. It is important to provide clear, firm, and unambiguous protection against any uses that would compromise or invade personal privacy.

This Memorandum establishes new procedures and provides updated guidance and requirements for agency use of web measurement and customization technologies. The central goal is to respect and safeguard the privacy of the American public while also increasing the Federal Government's ability to serve the public by improving and modernizing its activities online. Any use of such technologies must be respectful of privacy, open, and transparent, and solely for the purposes of improving the Federal Government's services and activities online.

For agency questions about this Memorandum, agencies should contact OMB at infopolicy-oira@omb.eop.gov.

Thank you for your cooperation.

Attachments

Attachment 1

Principles for Federal Agency Use of Web Measurement and Customization Technologies

1. **General.**

Scope and applicability. This guidance applies to any Federal agency use of web measurement and customization technologies. This guidance is not limited to any specific technology or application (such as persistent cookies), and it includes Federal agency use of third-party web measurement and customization technologies. Whenever an agency uses third-party websites or applications to engage with the public, it should refer to OMB's memorandum providing *Guidance for Agency Use of Third-Party Websites and Applications*.[3] In some cases, the third-party websites or applications use web measurement and customization technologies solely for the third party's own purposes. This guidance does not apply as long as (1) third parties do not use web measurement and customization technologies on behalf of a Federal agency, and (2) Personally Identifiable Information (PII), or any information that could be used to determine an individual's online activity derived from such uses, is not shared with the agency. However, agencies must consider the risk posed by such arrangements as part of the Privacy Impact Assessment required in OMB's memorandum providing *Guidance for Agency Use of Third-Party Websites and Applications*.

This guidance does not apply to internal agency activities (such as on intranets, applications, or interactions that do not involve the public) or to activities that are part of authorized law enforcement, national security, or intelligence activities.

Modifications to current guidance. This Memorandum rescinds OMB Memorandum M-00-13, *Privacy Policies and Data Collection on Federal Web Sites*, and the specified sections in the following memorandum:

- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*: Section III(D)(2)(v) concerning tracking and customization activities, and Section VII(B) regarding the reporting of tracking technologies.

2. **Definitions.**

Web measurement and customization technologies. These technologies are used to remember a user's online interactions with a website or online application in order to conduct measurement and analysis of usage or to customize the user's experience.

[3] OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications* (June 25, 2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf

Single-session technologies. These technologies remember a user's online interactions within a single session or visit. Any identifier correlated to a particular user is used only within that session, is not later reused, and is deleted immediately after the session ends.

Multi-session technologies. These technologies remember a user's online interactions through multiple sessions. This approach requires the use of a persistent identifier for each user, which lasts across multiple sessions or visits.

Personally Identifiable Information (PII). This term, as defined in OMB Memorandum M-07-16,[4] refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.

3. **Appropriate Use and Prohibitions.** Subject to the limitations described below, agencies may use web measurement and customization technologies for the purpose of improving Federal services online through conducting measurement and analysis of usage or through customization of the user's experience.

   Under no circumstances may agencies use such technologies:

   a. to track user individual-level activity on the Internet outside of the website or application from which the technology originates;

   b. to share the data obtained through such technologies, without the user's explicit consent, with other departments or agencies;

   c. to cross-reference, without the user's explicit consent, any data gathered from web measurement and customization technologies against PII to determine individual-level online activity;

   d. to collect PII without the user's explicit consent in any fashion; or

   e. for any like usages so designated by OMB.

4. **Usage Tiers.** Below are the defined tiers for authorized use of web measurement and customization technologies.

[4] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), *available at* http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf

a. **Tier 1 – single session.** This tier encompasses any use of single session web measurement and customization technologies.

b. **Tier 2 – multi-session without PII.** This tier encompasses any use of multi-session web measurement and customization technologies when no PII is collected (including when the agency is unable to identify an individual as a result of its use of such technologies).

c. **Tier 3 – multi-session with PII.** This tier encompasses any use of multi-session web measurement and customization technologies when PII is collected (including when the agency is able to identify an individual as a result of its use of such technologies).

5. **Clear Notice and Personal Choice.** Agencies must not use web measurement and customization technologies from which it is not easy for the public to opt-out. Agencies should explain in their Privacy Policy the decision to enable web measurement and customization technologies by default or not, thus requiring users to make an opt-out or opt-in decision. Agencies must provide users who decline to opt-in or decide to opt-out with access to information that is comparable to the information available to users who opt-in or decline to opt-out.

   a. **Agency side opt-out.** Agencies are encouraged and authorized, where appropriate, to use web tracking and measurement technologies in order to remember that a user has opted out of all other uses of such technologies on the relevant domain or application. Such uses are considered Tier 2.

   b. **Client side opt-out.** If agency side opt-out mechanisms are not appropriate or available, instructions on how to enable client side opt-out mechanisms may be used. Client side opt-out mechanisms allow the user to opt out of web measurement and customization technologies by changing the settings of a specific application or program on the user's local computer. For example, users may be able to disable persistent cookies by changing the settings on commonly used web browsers. Agencies should refer to http://www.usa.gov/optout_instructions.shtml, which contains general instructions on how the public can opt out of some of the most commonly used web measurement and customization technologies.

   c. **Tier 3 restrictions.** Agencies employing Tier 3 uses must use opt-in functionality.

6. **Data Safeguarding and Privacy.** All uses of web measurement and customization technologies must comply with existing policies with respect to privacy and data safeguarding standards. If applicable, agencies must cite the appropriate Privacy Impact Assessment (PIA) and/or System of Records Notice (SORN) in their online Privacy Policy.

a. **Comparable information and services.** If agencies are using a website or application hosted on a third-party site using web measurement and customization technologies to which Federal privacy and data safeguarding standards do not apply, they should provide the public with alternatives for acquiring comparable information and services. For example, members of the public should be able to learn about the agency's activities or to communicate with the agency without having to join a third-party social media website. If the third-party service is used to solicit feedback, agencies should provide an alternative government email address where users can also send feedback.

7. **Data Retention Limits and Access Limits.** Agencies may retain data collected from web measurement and customization technologies for only as long as necessary to achieve the specific objective for which it was collected. Moreover, only employees who need to have access to the data should be allowed to do so.

   a. **Retention time.** The time frame for retention of data must be both limited and correlated to a specific objective. If not required by law, policy, or a specific need for the web measurement or customization objective, agencies should limit the retention of such data to one year or less.

   b. **Records disposition schedule.** Information collected from web measurement and customization technologies that is determined to be a Federal Record must comply with Federal Records Act regulations. General Records Schedule 20 (GRS 20) pertains to Electronic Records; specifically, the disposition authority cited in General Record Schedule 20 Item 1C, "Electronic Records" ("*Files/Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records - Electronic files ... created to monitor system usage…*") is applicable to information collected from web measurement and customization technologies.[5] Use of GRS 20 is mandatory for those categories of electronic records described in the schedule unless the agencies have requested an alternative disposition authority from the National Archives and Records Administration.

8. **Enforcement.** To the extent feasible, technical enforcement mechanisms should be put in place to implement stated retention times and to limit access to authorized personnel. Where technical enforcement mechanisms are not feasible, policy or contractual enforcement mechanisms must be present.

9. **Verification.** Agencies using web measurement and customization technology must annually review their systems and procedures to demonstrate that they are in compliance with this policy. The results of this review shall be posted on the agency's "/open" page

[5] National Archives and Records Administration, *Electronic Records, General Record Schedule 20* (2010), *available at* http://www.archives.gov/records-mgmt/grs/grs20.html

located at www.[agency].gov/open,[6] with a mechanism for the public to provide feedback on the results.

Attachment 2

Process for Agency Use of Web Measurement and Customization Technologies

1. **Privacy Policy.** Federal agencies using web measurement and customization technologies in a manner subject to Tier 1 or Tier 2 are authorized to use such technologies so long as the agencies (1) are in compliance with this Memorandum and all other relevant policies; (2) provide clear and conspicuous notice in their online Privacy Policy citing the use of such technologies, as specified in Attachment 3; and (3) comply with their internal policies governing the use of such technologies.

2. **Privacy Office Review.** Any proposals by the agency to engage in Tier 3 uses must be reviewed by the Senior Agency Official for Privacy (SAOP).[7]

3. **Notice and Comment.** Following SAOP review, for new proposals of Tier 3 uses or substantive changes to existing uses of such technologies, agencies must:

    a. Solicit comment through their Open Government Webpage at www.[agency].gov/open for a minimum of 30 days. This notice and comment must include the agency's proposal to use such technologies and a description of how they will be used, which should at a minimum address the items in the Privacy Policy as described in Attachment 3; and

    b. Review and consider substantive comments and make changes to their intended use of web measurement and customization technologies where appropriate.

    With written approval from a Chief Information Officer (CIO), agencies are exempt from this requirement if the notice-and-comment process is reasonably likely to result in serious public harm.

4. **Tier 3 Review.** Agencies using web measurement and customization technologies in a manner subject to Tier 3 must have explicit written approval from their CIO. This approval must be cited in the agency's online Privacy Policy. After this approval has been obtained and after notice and comment, as specified in (3) above, has been completed, agencies are authorized to use Tier 3 web measurement and customization technologies.

5. **Previous Authorization for Use of Web Measurement and Customization Technologies.** Agencies that have received approval from their agency head under

[6] *See* OMB Memorandum, M-10-06, *Open Government Directive* (Dec. 8, 2009) (requiring each agency to create a "/open" webpage), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf

[7] OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy* (Feb. 11, 2005), *available at* http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf

previous guidance to use web measurement and customization technologies, or similar technologies, must bring their previous use of such technologies into compliance with this Memorandum within four months of the date of its publication.

6. **Unauthorized Use.** If any agency is found to be using web measurement and customization technologies outside of the process or parameters specified in this Memorandum, the agency must immediately cease use of such technologies and inform OMB of the extent of such unauthorized use. OMB will respond as necessary and appropriate.

Attachment 3

Required Additions to the Agency Privacy Policy when Web Measurement and Customization Technologies are Used

The following items must be added as part of the agency's online Privacy Policy, if they are not present, in any instance when web measurement and customization technologies are used:

i. the purpose of the web measurement and/or customization technology;

ii. the usage Tier, session type, and technology used;

iii. the nature of the information collected;

iv. the purpose and use of the information;

v. whether and to whom the information will be disclosed;

vi. the privacy safeguards applied to the information;

vii. the data retention policy for the information;

viii. whether the technology is enabled by default or not and why;

ix. how to opt-out of the web measurement and/or customization technology;

x. statement that opting-out still permits users to access comparable information or services; and

xi. the identities of all third-party vendors involved in the measurement and customization process.