



Privacy Impact Assessment

For

Impact Evaluation of Race to the Top and School Improvement Grants

Date: August 22, 2012

Point of Contact: Dr. Thomas Wei

(202) 208-0452

Thomas.Wei@ed.gov

System Owner: Dr. Audrey Pendleton

(202) 208-7078

Audrey.Pendleton@ed.gov

Author: Dr. Thomas Wei

(202) 208-0452

Thomas.Wei@ed.gov

Institute of Education Sciences

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.**

The system name is the “Impact Evaluation of Race to the Top and School Improvement Grants.” The system of records will contain records on students in tested grades from approximately 61 school districts in 21 states and the District of Columbia, and will be used to conduct a study evaluating the implementation and impacts of two of the Department of Education’s (Department) grant programs: Race to the Top and Title I School Improvement Grants.

- 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 study is authorized under the Education Sciences Reform Act of 2002, Part D, Section 171(b)(2) (20 U.S.C. 9561(b)(2)), which authorizes the Institute of Education Sciences to “conduct evaluations of Federal education programs administered by the Secretary (and as time and resources allow, other education programs) to determine the impact of such programs (especially on student academic achievement in the core academic areas of reading, mathematics, and science).” The collection of information is regulated by the Education Sciences Reform Act of 2002, the Privacy Act of 1974, and the Family Educational Rights and Privacy Act.

- 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?**

The system will contain records on students in tested grades from approximately 61 school districts in 21 states and the District of Columbia. This student-level information will include, but will not necessarily be limited to student IDs, the names and IDs of the school and school district that the student attends, year of birth, demographic information such as race, ethnicity, gender, and educational background (grade level, free and reduced-price lunch status, English language learner status, and special education status), whether the student graduated from high school and enrolled in college, and assessment information and scores on reading and mathematics state assessments. The sources of information are from state and/or district administrative records and will be collected and maintained in secure electronic form that complies with all federal security requirements (see response to question 11).

- 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.**

This information is being collected for statistical purposes. The central purpose and reason why the Department is establishing this system of records is to evaluate the implementation and impact of two of the Department’s grant programs: Race to the Top and Title I School Improvement Grants. In particular, we will address the following four research questions:



(1) How are Race to the Top and School Improvement Grants implemented at the state, district, and school levels? (2) Are Race to the Top reforms related to improvement in student outcomes? (3) Does receipt of School Improvement Grants funding to implement a school turnaround model have an impact on outcomes for low-performing schools? (4) Is the implementation of school turnaround models, and strategies within those models, related to improvement in student outcomes? The privacy risks from this system include any adverse consequences, such as embarrassment, to students from having their privacy-protected information used and disclosed in unauthorized ways. To mitigate these risks, the system establishes strict rules, procedures and security requirements related to the collection, maintenance, use, disclosure, and destruction of the student data that are outlined in responses to other questions in this Privacy Impact Assessment (PIA) and in the System of Records Notice (SORN), which together will protect the sensitive student data collected for the purposes of this study from unauthorized use and disclosure.

- 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.**

This system does not collect SSNs.

- 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.**

The intended use of the information is to evaluate the implementation and impact of two of the Department's grant programs: Race to the Top and Title I School Improvement Grants. See response to question 4 for more information on the specific research questions that the information will be used to address. See response to question 7 for information on internal and/or external uses and sharing of the information. The system will include individual student-level data from tested grades with personally identifiable information collected from existing state and/or district administrative records from approximately 61 school districts in 21 states and the District of Columbia. To analyze the data and generate findings that meet Institute of Education Sciences research standards, quantitative statistical methods will be used, such as regression discontinuity techniques. These analyses will produce an estimate of aggregate impacts from these two Department programs on the study sample of student outcomes.

- 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?**

The Department may disclose information contained in a record in this system of records under the routine uses listed in this system of records without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. Any disclosure of individually identifiable information from a record in this system must comply with the requirements of section 183 of the Education Sciences Reform Act (ESRA) (20 U.S.C. 9573), which provides confidentiality standards that apply to all collection, reporting, and publication of data by IES.



(1) Research Disclosure. The Director of IES may license de-identified confidential information from this system of records to qualified external researchers solely for the purpose of carrying out specific research that is compatible with the purpose(s) of this system of records. The researcher shall be required to maintain the confidentiality of the licensed data and to use it only for statistical purposes. All licensing will be accomplished pursuant to the National Center for Education Statistics Licensing Program, described in the following website: <http://nces.ed.gov/statprog/instruct.asp>

(2) Contract Disclosure. If the Department contracts with an entity to perform any function that requires disclosing records in this system to the contractor's employees, the Department may disclose the records to those employees who have received the appropriate level of security clearance from the Department. Before entering into such a contract, the Department will require the contractor to establish and maintain the safeguards required under the Privacy Act (5 U.S.C. 552a(m)) with respect to the records in the system.

- 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?**

See response to question 7.

- 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?**

A Privacy Notice on data collection forms that meets the requirements of the Privacy Act, 5 U.S.C. 552a(e)(3), is not required in this study since identifying information is being collected from the school district or state, not *directly from the students* for this system. School districts and states receiving American Recovery and Reinvestment Act funds will be informed of their obligation to respond to the data collection in order to obtain or retain a benefit under the Education Department General Administrative Regulations (34 C.F.R. § 76.591).

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

None; see response to question 9.

- 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?**

All physical access to the Department's site and to the sites of the Department's contractor and subcontractors, where this system of records is maintained, is controlled and monitored by security personnel. The computer system employed by the Department offers a high degree of resistance to tampering and circumvention. This security system limits data access to Department and contract staff on a need-to-know basis and controls individual users' ability to access and alter records within the system. The contractor and subcontractors will



establish a similar set of procedures at their sites to ensure confidentiality of data. The contractor and subcontractors are required to ensure that print data identifying individuals are in files physically separated from other research data and electronic files identifying individuals are separated from other electronic research data files. The contractor and subcontractors will maintain security of the complete set of all master data files and documentation. Access to individually identifying data will be strictly controlled. At each site, all print data will be kept in locked file cabinets during nonworking hours and work on hardcopy data will take place in a single room, except for data entry. Physical security of electronic data will also be maintained. Security features that protect project data include: password-protected accounts that authorize users to use the contractor's system but to access only specific network directories and network software; user rights and directory and file attributes that limit those who can use particular directories and files and determine how they can use them; and additional security features that the network administrators will establish for projects as needed. The Department's, contractor's, and subcontractors' employees who "maintain" (collect, maintain, use, or disseminate) data in this system must comply with the requirements of the Privacy Act and the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573), which provides criminal penalties for violations.

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 system is covered under the system of records notice entitled Impact Evaluation of Race to the Top and School Improvement Grants, dated October 12, 2012, (77 FR 62228-62231).

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:

Records are maintained and disposed of in accordance with the Department's Records Disposition Schedules ED 068.a (NARA Job Number: N1-441-08-18).