UNITED STATES DEPARTMENT OF EDUCATION
OFFICE OF INSPECTOR GENERAL

AUDIT SERVICES

March 15, 2018

Control Number
ED-OIG/A02O0008

Dr. Thomas W. Brock
Commissioner, National Center for Education Research
Delegated the Duties of the Director of Institute of Education Sciences
550 12th St. SW
Washington, D.C. 20202

Dear Dr. Brock:

This final audit report, "Protection of Personally Identifiable Information in Statewide Longitudinal Data Systems," presents the results of our audit. The purpose of the audit was to (1) assess the adequacy of the Institute of Education Sciences' (IES) Statewide Longitudinal Data System (SLDS) grant requirements and monitoring of States to ensure internal controls are in place to prevent, detect, and report unauthorized access and disclosure of personally identifiable information in SLDSs; and (2) determine whether selected States have internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in their SLDSs. Our review covered the internal controls in place from April 2005 through October 2017.

BACKGROUND

IES administers the SLDS grant program and monitors grantees' progress toward meeting the final goals of their approved grant applications. The grant program supports the design, development, and implementation of statewide longitudinal data systems that link individual student data across time and across databases. The long-term goal of the grants is to enable States to create comprehensive early learning through workforce data systems that will enhance their ability to efficiently and accurately manage, analyze, and use education data. The SLDSs are supposed to permit the facilitation of research to improve student academic achievement. The data in these systems can include personally identifiable information such as names, dates of birth, and Social Security numbers. The systems can also include performance data for major U.S. Department of Education (Department) programs such as Title I, Part A of the Elementary and Secondary Education Act and Part B of the Individuals with Disabilities Education Act. IES awarded at least one SLDS grant to 47 States, the District of Columbia, and three U.S. territories during the six competitions that it held between 2006 and 2015, with 39 of the 51 grantees receiving two or more grants.

Statewide Longitudinal Data System Grants

The purpose of the fiscal year (FY) 2006 grant was to support the design, development, and implementation of statewide longitudinal data systems to satisfy Federal, State, and local reporting requirements and meet the informational needs for data-driven decision-making at the State, district, school, classroom, and student levels. Grants awarded subsequent to the FY 2006 grant supported SLDS grantees in the design, development, and implementation of kindergarten through grade 12 (K–12) SLDSs. The grants could also be used to expand K–12 systems to include early childhood data, postsecondary data, and workforce data and to match teachers to students. States had to assure that they would protect student data and individual privacy consistent with applicable Federal and State requirements.

In the grant competition for FY 2015, IES shifted its focus to using the data that had been linked in previous grant rounds. Specifically, applicants who applied for funding were to carry out projects to address up to two of the following data use priorities: (1) Financial Equity and Return on Investment, (2) Educator Talent Management, (3) Early Learning, (4) College and Career, (5) Evaluation and Research, and (6) Instructional Support. States were to consider how their proposals would enhance their ability to use their SLDSs to address the needs of at-risk students under any of these priorities.

Institute of Education Sciences Monitoring

IES monitors SLDS grantees using bimonthly monitoring calls, site visits, and reviews of grantees' Annual Performance Reports (APR) and Final Performance Reports (FPR). The APRs and FPRs summarize the grant project's progress, problems, proposed solutions, and budget. The project plan section lists a grantee's proposed outcomes from the grant application along with their status, actual or projected start and end dates, and comments. IES monitors the project plan portion of the APR to ensure the projects are meeting their goals and timeframes. In addition, IES conducts a risk analysis using its Risk Management and Monitoring worksheet, which includes information found in the grantees' APRs and FPRs and also takes into consideration grantees' participation in required monitoring activities. The Risk Management and Monitoring worksheet analyzes financial, management, and performance indicators to arrive at a low, at-risk, or significant risk level. Some indicators include total grant award amount, timely expenditures, staff capacity, and a grantee's progress towards goals listed in its project plan. The risk analysis determines the frequency of site visits that IES will conduct on each grantee. According to the IES document "Site Visit Guiding Questions," areas of focus during the monitoring visit include (1) project history and background, (2) project governance, (3) data governance, (4) data use, (5) stakeholder group meetings, and (6) sustainability.

Privacy Technical Assistance Center

The Privacy Technical Assistance Center (PTAC), which is administered by the Department through a contract, serves as a resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC performs the following activities: (1) operates a help desk and answers questions on privacy concerns; (2) provides general technical assistance for stakeholders, including developing issue briefs, white papers, case studies, online resources, and classroom- and computer-based training; and (3) provides targeted technical assistance on request, including site visits, reviews of data sharing agreements and memorandums of understanding, and conference presentations.

AUDIT RESULTS

To answer our objectives, we reviewed IES's SLDS grant requests for applications; three State grantees' approved grant applications; IES's monitoring policies and procedures used to ensure grantees met grant requirements; and internal controls to prevent, detect, and report unauthorized access and disclosure of personally identifiable information in SLDSs. In addition, we reviewed the internal controls at three selected State grantees to determine whether grantees met grant requirements and had internal controls to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in their SLDSs.

We found that IES's grant requirements were adequate to ensure the protection of personally identifiable information. Specifically, both the IES SLDS grant requests for applications and the approved grant applications stated that the grantees would meet applicable Federal and State laws or regulations concerning the confidentiality of individual records. Applicants were also required to demonstrate that they met or would meet technical requirements concerning data quality, with the grant requests for applications stating that a successful data system must ensure the integrity, security, and quality of data. We found that the grantees that we audited addressed these requirements in the approved grant applications by identifying and noting that they would comply with specific State requirements pertaining to data and system security. However, we found that IES had inadequate controls for monitoring its grantees' adherence to State system security requirements. Specifically, IES did not ensure that its grantees met the minimum State system security requirements of their respective States as required by the SLDS grant assurances that they provided as a condition of receiving grant funds. We identified internal control weakness at all three grantees audited that increased the risk that these grantees would be unable to prevent or detect unauthorized access and disclosure of personally identifiable information in their SLDSs. [1]

In its comments on the draft report, IES generally concurred with our finding and concurred with our recommendations. IES acknowledged that it did not monitor grantees' compliance with their State system security laws and regulations concerning the confidentiality of individual records and provided a corrective action plan to address the recommendations. Based on IES's comments, we made minor changes to the report for clarification. We summarized IES's comments at the end of the finding and included the full text of its comments as Attachment 2 of this report.

[1] "The Protection of Personally Identifiable Information in the Commonwealth of Virginia's Longitudinal Data System," (ED-OIG/A02P006), July 12, 2016; available at https://www2.ed.gov/about/offices/list/oig/auditreports/fy2016/a02p0006.pdf.
"The "The Protection of Personally Identifiable Information in Oregon's Statewide Longitudinal Data System," (ED-OIG/A02P0007), September 27, 2016; available at https://www2.ed.gov/about/offices/list/oig/auditreports/fy2016/a02p0007.pdf.
"The Protection of Personally Identifiable Information in Indiana's Statewide Longitudinal Data System," (ED-OIG/A06Q0001), July 10, 2017; available at https://www2.ed.gov/about/offices/list/oig/auditreports/fy2017/a06q0001.pdf.

FINDING – The Institute of Education Sciences Did Not Monitor SLDS Grantees' Compliance with State System Security Requirements

We found that IES lacked controls to ensure that SLDS grantees followed grant requirements regarding the protection of personally identifiable information in their SLDSs. The requests for applications required grantees to agree that they would follow all applicable Federal and State laws or regulations concerning the confidentiality of individual records and also demonstrate that they met or would meet technical requirements concerning data integrity, security and quality. However, IES did not include as part of its monitoring procedures a determination on whether its grantees met the minimum State system security requirements identified in their applications.

IES Did Not Monitor for SLDS Security Controls

IES did not ensure that grantees followed their State laws and regulations concerning the prevention and detection of unauthorized access and disclosure of personally identifiable information in SLDSs. This occurred because IES did not include steps in its monitoring procedures to review for grantees' compliance with State laws and regulations regarding system security. We reviewed IES's monitoring procedures, which required that program staff review grantees' APRs and FPRs and develop Risk Management and Monitoring worksheets and conduct site visits. We also reviewed available monitoring documentation for the three grantees that we audited to determine whether program staff considered grantees' adherence to State system security laws and regulations. Grantees were not required to report on their adherence to State laws or regulations regarding system security, and we noted, for the three grantees that we audited, only 2 of the 28 APRs and FPRs provided information on the State's adherence to this requirement. Further, Risk Management and Monitoring worksheets and site visit reports that we reviewed never mentioned adherence to State laws and regulations regarding system security. The IES research scientist team lead[2] confirmed that IES does not monitor whether grantees are following State laws and regulations regarding system security.

Although IES's monitoring procedures did not include steps to check for grantees' compliance with State system security laws and regulations, we found that both IES and PTAC provided technical assistance to grantees regarding system security. For example, some of the technical and best practice guidance offered on IES's website included "Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records," "Basic Concepts And Definitions for Privacy And Confidentiality in Student Education Records," "Technical and Business Documentation for an SLDS," and "Working with a Central State IT Agency to Develop an SLDS." The best practice brief "Technical and Business Documentation for an SLDS" discusses documenting a system security plan as well as "processes and procedures that are used to develop and maintain a data security program to include consistency with program laws, statutes, and regulations." The best practice brief "Working with a Central State IT Agency to Develop an SLDS" noted the importance of "[t]echnical controls such as role-based access, security logs, and audits" to help ensure compliance with applicable requirements "for tracking where education records go and who has access to them." In addition, IES used PTAC to assist grantees in securing their SLDSs. PTAC provided guidance on areas such as identifying all personally identifiable and sensitive information, role-based access to student record data, and responding to breaches of personally identifiable information. PTAC provided assistance to grantees upon request.

[2] This research scientist monitors SLDS grantees and manages the other research scientist.

The IES audit liaison[3] expressed concern over IES's ability to oversee the various grantees' State system security laws and regulations. The IES research scientist team lead stated that to address State system security laws and regulations going forward, IES plans to make changes to its site visit protocol and APR instructions for grantees and has added technical assistance including best practices on protecting students' personally identifiable information and securing State systems. However, we noted that its current FY 2015 grant "Site Visit Guiding Questions" document did not state how IES would ensure grantees' compliance with State system security requirements. Also, although IES provided the APR instructions for the June 30, 2017, submissions, these instructions ask only whether the grantee is aware of its State and local data security and student privacy regulations; grantees must provide support that they are complying with State laws and regulations only if IES requests it.

According to the Department's "Handbook for the Discretionary Grant Process," IES is responsible for ensuring that grantee projects adhere to laws, regulations, conditions of the grant, certifications, and assurances. In addition, according to the Government Accountability Office's "Standards for Internal Control in the Federal Government," September 2014, management should design control activities in response to the entity's objectives and risks to achieve an effective internal control system. The IES SLDS grant requests for applications required that the applicant's SLDS must ensure the confidentiality of student data is consistent with the requirements of Federal and State laws or regulations concerning the confidentiality of individual records and also comply with technical requirements concerning data quality, which encompasses both data integrity and security. Applicants were to identify that these requirements were in place, and if the requirements were not currently in place, describe how they would be developed throughout the grant. All three of the selected grantees we reviewed stated in their grant applications that their SLDSs would be in compliance with State system security laws and regulations; however, none of the grantees described how the requirements would be developed.

Because IES did not monitor to ensure that SLDS grantees met grant requirements regarding the protection of personally identifiable information, it was unaware that grantees did not meet the minimum system security requirements found in each of their State laws and regulations. All of the grant applications for the three States that we audited stated that the grantee would meet the required State laws and requirements concerning system security. However, we found that none of the three grantees met minimum State system security requirements. We identified internal control weaknesses in the SLDSs for the Virginia Department of Education (VDOE), Oregon Department of Education (ODE), and Indiana Department of Education (IDOE) that increased the risk that these grantees will be unable to prevent or detect unauthorized access and disclosure of personally identifiable information. Further, because IES did not monitor grantees' adherence to State laws and regulations regarding system security for their SLDSs while the grants were active, grantees may be at an increased risk of a breach.

SLDSs at Selected States Did Not Comply with State System Security Requirements

VDOE was not in compliance with grant requirements covering system security. We found that VDOE did not ensure its SLDS, which VDOE classified as sensitive, met required State standards for sensitive systems. A May 2014 information technology audit by Virginia's Information Technology Agency cited issues with all system control areas identified in

[3] The audit liaison is a management and program analyst who served as our liaison.

Virginia's State standards. A June 2014 audit by the Auditor of Public Accounts identified additional missing system controls in five system control areas in VDOE's SLDS that did not meet the minimum State standards. We reviewed VDOE's System Security Plan and a corrective action plan that addressed both of these audits. Based on our review of the corrective action plan, the System Security Plan, and VDOE's policies and procedures, VDOE had not adequately addressed the Virginia Information Technology and Auditor of Public Accounts audit findings to ensure that its system controls met the minimum State standards. In its fiscal year 2009 SLDS grant application, VDOE stated that it would implement security controls in accordance with Virginia's Information Security Standards.

ODE was not in compliance with its SLDS grant requirements covering system security. We found that ODE did not ensure that its SLDS met the minimum requirements in Oregon's State standards. Specifically, ODE did not develop and implement an Information Security Plan, conduct annual risk assessments, and classify the security levels of its SLDS as required by State standards. In its fiscal year 2007 and 2009 SLDS grant applications, ODE stated that it would ensure the confidentiality of student records by following Oregon Revised Statutes and Oregon Administrative Rules.

IDOE was not in compliance with its SLDS grant requirements covering system security. We found that IDOE did not ensure that its SLDS met the minimum requirements in Indiana's State standards. Specifically, IDOE did not ensure that its SLDS had a System Security Plan, underwent a compliance audit and a risk assessment, and had its security level classified. Also, the IDOE data warehouse, a K–12 system that feeds data to the SLDS, did not meet the minimum State security requirements. Specifically, IDOE had no written policies and procedures for the protection of personally identifiable information in its data warehouse. In its fiscal year 2012 SLDS grant application, IDOE stated that it would ensure the confidentiality of student records by following all applicable Federal and State privacy laws. However, we found that IDOE was not aware of some of its State system security requirements.

IES has not resolved the audit findings and recommendations for two of the three issued State audit reports by the required deadlines. Office of Management and Budget's Circular A-50 requires prompt resolution and corrective actions on audit recommendations, with resolution within a maximum of 6 months after issuance of a final report. IES indicated that because the grants were closed, it did not feel that it had the ability to require States to take corrective actions to ensure that their systems were secure. However, the Office of Management and Budget's Uniform Guidance, at Title 2 Code of Federal Regulations (C.F.R.) Part 200 supports efforts to secure corrective action by these States even after grant closeout. To remedy a grantee's noncompliance with the terms and conditions of a Federal award, Title 2 C.F.R. § 200.338 provides that the Federal awarding agency may disallow all or part of the cost of the activity or action not in compliance, withhold further Federal awards for the project or program, or take other remedies that may be legally available.[4] Title 2 C.F.R. § 200.344, states that "the closeout of a Federal award does not affect … (a) the right of the Federal awarding agency … to disallow costs and recover funds on the basis of a later audit or other review … within the record retention

[4] The Uniform Guidance in Title 2, C.F.R., replaced Title 34, C.F.R., for new and continuation awards that the Department issued on or after December 26, 2014. The Uniform Guidance was not in effect when these SLDS grants were awarded; however, the same requirements mentioned for Title 2 C.F.R. §200.338 and Title 2 C.F.R. §200.344(a) are found in Title 34 C.F.R. §74.62 and Title 34 C.F.R. §74.72(a) respectively which were in effect when these SLDS grants were awarded.

period." In addition, per Title 34 C.F.R. § 75.217(d)(ii), in deciding whether to make future awards to an applicant, the Department considers the applicants performance under a previous Department award.

In June 2017, the IES audit liaison stated that IES was initially having difficulty getting a response from VDOE and ODE on the corrective actions for our respective audits. However, the IES audit liaison added that VDOE and ODE are now cooperating with IES to resolve the issues identified in the audits. In July 2017, the Office of the Chief Financial Officer became the primary office responsible for the resolution of these audits, with IES as the secondary office.

Since IES did not ensure that VDOE, ODE, and IDOE implemented minimum State system security requirements while their grants were active and does not yet have assurances that the States have taken steps to protect the confidentiality of individual student records, these grantees' SLDSs may still be vulnerable to a breach. Until IES incorporates monitoring procedures to oversee compliance with State system security requirements, it will not be fully aware as to whether or not grantees' SLDSs meet State standards. As such, personally identifiable information in these SLDSs may be at an increased risk to unauthorized access and disclosure.

Recommendations

We recommend that the Commissioner of the National Center for Education Research, who has been delegated the duties of the IES Director—

1. Modify the SLDS program monitoring policies and procedures to include a review of SLDS grantees' compliance with State laws and regulations regarding system security and the protection of personally identifiable information.

2. Issue a Dear Colleague Letter to SLDS grantees emphasizing the importance of data security, and require grantees to positively affirm on their APRs and FPRs that their SLDSs are in compliance with State laws and regulations regarding system security and the protection of personally identifiable information.

3. Modify the SLDS program risk assessment and the risk-based monitoring process to include consideration of system security compliance issues.

IES Comments

In its comments on the draft audit report, IES generally concurred with our finding and provided a corrective action plan in response to our recommendations. IES's planned corrective actions, which will be completed between May and September 2018, include updating its monitoring protocols to include questions specific to grantees' compliance with State laws and regulations regarding system security and the protection of personally identifiable information, distributing a Dear Colleague Letter expressing the importance of data security and outlining new requirements in the SLDS APRs/FPRs, and specifying in its Risk Management and Monitoring worksheet that program officers should consider compliance with State laws and regulations regarding system security and the protection of personally identifiable information when determining the risk level of grantees. IES requested that the OIG clarify that grantees are required to comply with Federal and State laws or regulations concerning the confidentiality of individual records, and asked that we remove the broader references to information system security requirements. IES stated that although the confidentiality of individual records often depends on compliance with information

system security requirements, there may be other such requirements that do not fall within the SLDS grant requirements. IES acknowledged that it did not monitor grantees' compliance with their State laws and regulations concerning the confidentiality of individual records but believes that the monitoring and technical assistance provided ensured that grantees had effective protections in place for the protection of personally identifiable information. IES also stated that the grantees are required to demonstrate that they have a detailed data governance plan in place that IES monitors through site visits and monthly calls. Furthermore, IES stated it believes this level of on-site monitoring is necessary due to the complexity of the technical and security issues involved in linking data on individual students across data systems.

OIG Response

IES's planned corrective actions should address our recommendations, if implemented; however, we encourage immediate action when possible given the significant risks associated with any weaknesses in controls related to the protection of personally identifiable information. To address IES's comments regarding information system requirements, we clarified in this report that applicants were required to demonstrate that they met or would meet technical requirements concerning data integrity, security, and quality. In addition, we clarified that applicants were required to demonstrate that they met or would meet applicable Federal and State laws or regulations concerning the confidentiality of individual records. We have also noted, under the terms of the grants, the grantees we audited agreed to comply with specific State data and system security requirements. Although, we acknowledged that IES conducted monthly calls and site visits to include compliance with the grantee's data governance plan, these reviews did not identify the States failure to ensure their SLDSs met the State's data and system security requirements.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our audit objectives were to (1) assess the adequacy of IES's SLDS grant requirements and monitoring of States to ensure internal controls are in place to prevent, detect, and report unauthorized access and disclosure of personally identifiable information in SLDSs and (2) determine whether selected States have internal controls in place to prevent, detect, report, and respond to unauthorized access and disclosure of personally identifiable information in SLDSs. Our review covered the internal controls in place from April 2005 through October 2017.

To accomplish our objectives, we interviewed officials from IES and PTAC. Additionally, we reviewed:

- IES's organizational chart;
- IES site visit protocols and APR instructions for SLDS grantees;
- VDOE, ODE, and IDOE reports, including APRs, FPRs, Risk Management and Monitoring worksheets, and site visit reports;
- IES's SLDS Requests for Applications;
- VDOE, ODE, and IDOE approved SLDS grant applications;
- IES and PTAC technical assistance and guidance documents regarding system security;
- the Department's "Handbook for the Discretionary Grant Process;" and

- the following Government Accountability Office audit reports:
  - "Protecting Personally Identifiable Information" (GAO-08-343), January 2008;
  - "Alternatives Exist for Enhancing Protection of Personally Identifiable Information" (GAO-08-536), May 2008; and
  - "Challenges in Matching Student and Worker Information Raise Concerns about Longitudinal Data Systems" (GAO-15-27), November 2014.

We conducted an entrance conference with IES on February 11, 2015. The audit was subsequently placed on hold on February 26, 2015, while we conducted audits at our three selected grantees. We resumed the audit on January 3, 2017; we conducted fieldwork at IES's office in Washington, D.C., from January 31, 2017, through June 21, 2017. We held an exit conference with IES on October 26, 2017, to discuss the results of the audit.

We selected three States for a series of audits to assess how States' SLDSs protected personally identifiable information. We judgmentally selected VDOE, ODE, and IDOE based on the following characteristics: (1) total amount of SLDS funding, (2) status and extent of grant program participation, and (3) the State's number of reported education system data breaches.[5] We selected VDOE because it received more than $5 million in SLDS funding, had two SLDS grants that were closed, and the Identity Theft Resource Center reported that it had more than three breaches in its educational systems. In addition, we selected VDOE because IES stated that VDOE was a model State for protecting personally identifiable information in their SLDS. We selected ODE because it received more than $5 million in SLDS funding, two of its three grants were closed, and the Identity Theft Resource Center reported that it had three breaches related to its educational systems. We selected IDOE because it received more than $5 million in SLDS funding, one of its two grants was closed, and the Identity Theft Resource Center reported that it had three breaches related to its educational systems.

We assessed the internal controls designed by IES to ensure that grantees met grant requirements and had internal controls in place to prevent, detect, and report unauthorized access and disclosure of personally identifiable information in their SLDSs. We assessed IES's monitoring controls and technical assistance through inquiries of IES and PTAC personnel and review of written policies and procedures and various documentation, including monitoring reports. We found IES had inadequate controls for monitoring its grantees' adherence to State system security requirements, which we fully discuss in the audit finding.

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

[5] The data breaches included any education system breaches that the Identity Theft Resource Center reported. The breaches may not be specific to the SLDS. The Identity Theft Resource Center is a nonprofit organization that serves as a national resource on consumer issues related to cyber security, data breaches, social media, fraud, scams, and other issues.

ADMINISTRATIVE MATTERS

Statements that managerial practices need improvements, as well as other conclusions and recommendations in this report, represent the opinions of the Office of Inspector General. Determinations of corrective action to be taken will be made by the appropriate Department of Education officials.

Attached is the subject final audit report that covers the results of our review of IES's Protection of Personally Identifiable Information in Statewide Longitudinal Data Systems at IES during April 2005 through October 2017. An electronic copy has been provided to your Audit Liaison Officer. We received your comments concurring with the finding and recommendation in our draft report.

Corrective actions proposed (resolution phase) and implemented (closure phase) by your office will be monitored and tracked through the Department's Audit Accountability and Resolution Tracking System. The Department policy requires that you develop a final corrective action plan for our review in the automated system within 30 calendar days of the issuance of this report. The corrective action plan should set forth the specific action items, and targeted completion dates, necessary to implement final corrective actions on the finding and recommendations contained in this final audit report.

In accordance with the Inspector General Act of 1978, as amended, the Office of Inspector General is required to report to Congress twice a year on the audits that remain unresolved after six months from the date of issuance.

In accordance with the Freedom of Information Act (5 U.S.C. § 552), reports issued by the Office of Inspector General are available to members of the press and general public to the extent information contained therein is not subject to exemptions in the Act.

We appreciate the cooperation given us during this review. If you have any questions, please call Alyce Frazier at (646) 428-3871.

Sincerely,

/s/

Patrick J. Howard
Assistant Inspector General for Audit

Attachments

Attachment 1: Acronyms, Abbreviations and Short Forms Used in this Report

APR	Annual Performance Report
C.F.R.	Code of Federal Regulations
FPR	Final Performance Report
Department	U.S. Department of Education
FY	Fiscal Year
IDOE	Indiana Department of Education
IES	Institute of Education Sciences
K–12	Kindergarten through Grade 12
ODE	Oregon Department of Education
PTAC	Privacy Technical Assistance Center
SLDS	Statewide Longitudinal Data System
VDOE	Virginia Department of Education

Attachment 2: IES Comments on the Draft Report

UNITED STATES DEPARTMENT OF EDUCATION

Institute of Education Sciences

January 30, 2018

Patrick J. Howard
Assistant Inspector General for Audit
Office of Inspector General

Subject: Comments on draft audit report, "Protection of Personally Identifiable Information in Statewide Longitudinal Data Systems (Control Number ED-OIG/A02O0008)

Dear Mr. Howard:

Thank you for providing the Institute of Education Sciences (the Institute) with an opportunity to review and respond to the finding and recommendations in the Office of Inspector General's (OIG) draft audit report on "Protection of Personally Identifiable Information in Statewide Longitudinal Data Systems" (OIG Control Number ED-OIG/A02O0008). As Associate Commissioner for the division that oversees the program, I am responding on behalf of Thomas Brock, Commissioner for Education Research and Delegated the Duties of Director of the Institute.

Overview

The Educational Technical Assistance Act of 2002 established the Statewide Longitudinal Data System Grant Program (SLDS), which supports State Education Agencies' efforts to "design, develop, and implement statewide, longitudinal data systems to efficiently and accurately manage, analyze, disaggregate, and use individual student data." These systems often link student data across data systems and sectors, enabling States to create comprehensive early learning through workforce data systems, which will facilitate research to improve student academic and labor outcomes.

For each SLDS grant competition, project deliverables and grant requirements – including the requirement to ensure the confidentiality of student data, consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA), as well as any other applicable Federal and State laws or regulations concerning the confidentiality of individual records – are described in the Request for Applications (RFA). Applicants submit State Project Plans in response to the RFA and, if funded, the grantees update these State Project Plans to reflect their progress throughout the project period. The Institute awards SLDS grants as cooperative agreements, which provides additional flexibility for either party to amend the agreements if needed to ensure that grantees make sufficient progress towards the requirements and objectives in their State

Project Plans. Moreover, cooperative agreements allow for greater involvement in and oversight of the projects by the Institute. Grantees are monitored by Program Officers within the National Center for Education Statistics through monthly update calls with State SLDS teams, Annual Performance Reports (APRs), Final Performance Reports (FPRs), and regular site visits to grantees.

General Comments

We are pleased that this draft report acknowledges the steps that the Institute has taken to assist States on topics related to data security and privacy. For example, the report recognizes the SLDS program's collaboration with the Department's Privacy Technical Assistance Center (PTAC) to provide technical assistance to both grantee and nongrantee States regarding protections for student privacy and the confidentiality of individual records consistent with FERPA and other applicable Federal or State laws and regulations. The Institute has been instrumental in ensuring funding and continued guidance for PTAC's technical assistance in recent years. The draft report also notes that grantees are now required to indicate in their APRs whether they are aware of Federal and State laws or regulations concerning the confidentiality of individual records that are applicable to their grant activities, and that they must provide documentation regarding their compliance with these laws and regulations if requested by the Institute.

However, we believe that the report fails to acknowledge sufficiently that monitoring grantee compliance with State laws or regulations concerning individual records is not the only method available to the Institute to protect the confidentiality of personally identifiable information. In their applications, SLDS grantees are required to demonstrate that they have a detailed data governance plan in place. This is critical in order to ensure that only individuals who should have access to data (based on Federal, State, and local policy) can access those data and that the data are used in acceptable ways. Program officers monitor grantee compliance with the data governance plan through monthly calls and site visits. Site visits occur, on average, at least every 18 months or more often if a grantee is determined to be at high risk of not meeting its project requirements and deliverables. The Institute believes that this level of on-site monitoring is necessary because of the complexity of the technical and security issues involved in linking data on individual students across data systems.

All grantees that are using individual student data, either for reports and research or by merging cross sector data, are also required to comply with Federal requirements for the protection of human subjects in research supported by the Department. These requirements include providing documentation that these planned activities have been reviewed and approved by an Institutional Review Board. Program officers in the Institute work closely with the Department's Human Subjects Officer in the Office of the Chief Financial Officer to ensure grantees are complying with these requirements.

To date, grantees have reported no breaches of data involving information or records managed with funds from the SLDS program. We do not take the risk of unauthorized access to or disclosure of personally identifiable information lightly. We strongly urge SLDS grantees and all States and districts to participate in simulations and trainings designed to help them detect and

remediate unauthorized access and data breaches immediately. Grantees are not required by law to report data breaches to the Department, but we urge them to do so voluntarily so that PTAC and others in the Department can help them address the situation and mitigate the damage.

Our responses to the draft finding and recommendations are set forth below.

Finding: The Institute of Education Sciences Did Not Monitor SLDS Grantees' Compliance with State System Security Requirements.

The Institute generally concurs with this finding but notes that SLDS grantees are required to comply with "Federal and State laws or regulations concerning the confidentiality of individual records." Although the confidentiality of individual records often depends upon compliance with information system security requirements, there may be other system security requirements that do not fall within the SLDS grant requirements. We request that the OIG clarify this point and modify the findings and recommendations to reflect the requirement that grantees comply with Federal *and State* laws or regulations concerning the confidentiality of individual records, and remove the broader references to information system security requirements.

Although we believe our monitoring and technical assistance processes did ensure that grantees had effective protections for personally identifiable information in place, we acknowledge that we did not monitor grantee compliance with their State laws and regulations concerning the confidentiality of individual records.

Recommendation #1: Modify the SLDS program monitoring policies and procedures to include a review of SLDS grantees' compliance with State laws and regulations regarding system security and the protection of personally identifiable information.

The Institute concurs with this recommendation and has already taken steps to improve our efforts to monitor grantee compliance with State laws or regulations concerning the confidentiality of individual records. For example, we have amended our "Site Visit Guiding Questions" to ask grantees to describe the extent to which they are in compliance with their State's laws and regulations concerning the confidentiality of individual records, and have used the revised questions in site visits to Mississippi and Hawaii. These new items complement existing questions focused on ensuring compliance with applicable requirements concerning the treatment of human subjects and adherence to the grantee's data governance plan. The Institute will also revise its protocols for monthly monitoring calls as needed to assess grantee compliance with State laws and regulations concerning the confidentiality of individual records.

The Institute will continue to work with the PTAC to provide technical assistance to States on data security and privacy. In response to the issues identified in the course of this audit, the Institute invited the PTAC to conduct a session at the 2017 SLDS Best Practices Conference specifically to remind States of their obligation to understand and follow data security and privacy requirements and to help States understand the types of documentation they should be able to provide as evidence of compliance. While SLDS grantees are required to attend this annual conference, all States are invited and travel costs for staff from States without active SLDS grants are paid for by the Department. SLDS teams from 50 States and territories

attended the 2017 conference, and the Institute has invited the PTAC to provide similar technical assistance and guidance related to data security and privacy for both grantee and non-grantee States during the 2018 conference.[1]

Recommendation #2: Issue a Dear Colleague Letter to SLDS grantees emphasizing the importance of data security, and require grantees to positively affirm on their APRs and FPRs that their SLDSs are in compliance with State laws and regulations regarding system security and the protection of personally identifiable information.

The Institute concurs with this recommendation. To help grantees understand the importance of compliance with State laws or regulations concerning the confidentiality of individual records, we will distribute and post online a Dear Colleague letter, which will outline the new requirements within SLDS APRs and FPRs. It will also explain the importance of data security and will provide details about the technical assistance resources available to grantees through both the SLDS State Support Team and the PTAC.

Grantees are now required in their APRs to indicate whether they are aware of their State laws and regulations concerning the confidentiality of individual records. The APR indicates that, if requested by the Institute, grantees must provide evidence that they are complying with these State laws and regulations. The Institute will work with the PTAC to develop more detailed questions to assess grantee compliance with these laws or regulations and amend the APR, FPR, and review forms accordingly.

Recommendation #3: Modify the SLDS program risk assessment and the risk-based monitoring process to include consideration of system security compliance issues.

The Institute concurs with this recommendation. Program officers complete a Risk Management and Monitoring Worksheet as part of their review of grantees' APRs and other monitoring and performance information. Although this worksheet includes an assessment of whether the grantee has complied with the grant requirements, the examples provided do not currently include compliance with State laws and regulations concerning the confidentiality of individual records. The Institute will revise the worksheet to specify that program officers should consider compliance with this requirement when determining the risk level of SLDS grantees. The Institute will also host a webinar for current SLDS grantees to explain the changes to monitoring, APR and FRP requirements, and grantee risk level assessments.

As noted above, because the SLDS grant is a cooperative agreement, the Institute has the flexibility to amend cooperative agreements if the risk level assessment or other monitoring activities suggest that a grantee is at High Risk for not fulfilling the requirements and objectives of the project, including compliance with State laws or regulations concerning the confidentiality of individual records. In the past, grantees identified as being at High Risk have been

[1] This number includes representatives from the District of Columbia, the Commonwealth of the Northern Mariana Islands, Guam, Puerto Rico, and the US Virgin Islands. California, Iowa, New York, Oregon, and Wyoming chose not to send representatives to attend the conference.

recommended for increased monitoring and technical assistance, including, for example, on-site technical assistance visits, more frequent monitoring calls, and/or cost reimbursement.

Please let us know if you have any questions or need further information about any of our comments and responses. We appreciate the effort that went into the field work and the report and thank you for the opportunity to review and respond to the draft.

Sincerely,

Ross C. Santy, Jr.
Associate Commissioner
Administrative Data Division
National Center for Education Statistics
Institute of Education Sciences

cc: Thomas Brock

Enclosures