Office of Inspector General
Student Data

Report #A-1617-028 **January 2018**

Executive Summary

In accordance with the Department of Education's fiscal year (FY) 2016-2017 audit plan, the Office of Inspector General (OIG) conducted an audit of Student Survey Data administered by the Division of Technology and Innovation (DTI) through the Office of Education Information and Accountability Services (EIAS). The purpose of this audit was to determine whether Student Data meets standards for data reliability, validity, and security in accordance with state statute and rule.

During this audit, we noted that, in general, EIAS is meeting requirements for collecting, preparing, and storing Student Survey data in the state's Education Data Warehouse; and the data is valid and reliable for conducting Full-time Equivalent (FTE) calculations to facilitate the funding of Florida's public schools. We also noted EIAS is effectively conducting quality assurance activities on the submitted data. However, there were instances where DTI and EIAS could make improvements to strengthen controls. For example, we cited a need to strengthen internal controls for ongoing monitoring of system and user activity; establish documented policies for processing system overrides; and establish a Disaster Recovery Plan to strengthen the department's ability to recover time sensitive data. The Audit Results section below provides details of the instances noted during our audit.

Scope, Objectives, and Methodology

The scope of this audit included an analysis of Student Data Survey 2 collected and administered by the department's Division of Technology and Innovation through the Office of Education Information and Accountability Services during FY 2016-2017. We established the following objectives for our audit:

1. Determine whether the department has effective internal controls to ensure the valid and reliable collection of student data; and
2. Determine whether the department has effective security controls to protect student data from unauthorized access or modification.

To accomplish our objectives, we reviewed applicable laws, rules, and regulations; interviewed appropriate department staff; reviewed policies, procedures, and related documentation;

evaluated data collection procedures; tested edit checks; reviewed the quality assurance process; and reviewed system overrides.

Background

The Florida Department of Education's (department) office of PK-12 Education Information and Accountability Services (EIAS) serves to improve education by increasing the quality of decisions with data. Functions and services provided by EIAS include assisting school districts in the reporting of accurate information, providing information to customers in order to meet their needs, fulfilling the department's information database requirements, and reviewing and developing data collection procedures. EIAS collaborates with other divisions and offices to manage the collecting of student data for PK-12. These divisions and offices include the Division of Technology and Innovation (DTI), PK-20 Education Data Warehouse, and the Performance Accountability and Assessment Unit.

EIAS collects student data from each school district, juvenile justice education entity, virtual school, and charter school. The reporting entities submit their data through the State of Florida Northwest Regional Data Center (NWRDC). EIAS runs edit checks for collected survey data and monitors batch files for errors. The Florida Education Finance Program (FEFP) uses the data to calculate FTEs (Full-time equivalent) and funding levels. The department conducts eight surveys of school district students and staff information at scheduled times during the school year. The surveys are as follows:

- Surveys 1-4 are concurrent with the survey weeks specified by the Commissioner of Education and used for FTE reporting;
- Survey 5 is used to collect end of year information and secondary career and technical education information;
- Survey 6 is a beginning of the year student enrollment report and populates the FACTS.org system;
- Survey 8 populates the Progress Monitoring and Reporting Network system; and
- Survey 9 is used to collect information about students in schools for neglected and delinquent youth and information about Title I Supplemental Educational Services.

This audit focused on student data collected during Survey 2 of FY 2016-2017.

Audit Results

Finding 1: EIAS does not have internal controls to view user or system activity.

Florida Administrative Code (F.A.C.) Rule 74-2, the Florida Cybersecurity Standards, establishes cybersecurity standards for information technology (IT) resources. F.A.C. 74-2.003 (7) *Protective Technology* states, "Each agency shall ensure that technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. Specifically, each agency shall:
(a) Determine and document required audit/log records, implement logging of audit records, and protect and review logs in accordance with agency-developed policy. Agency-developed policy shall be based on resource criticality. Where possible, ensure that electronic audit records allow

actions of users to be uniquely traced to those users so they can be held accountable for their actions. Maintain logs identifying where access to exempt, or confidential and exempt data was permitted. The logs shall support unique identification of individuals and permit an audit of the logs to trace activities through the system, including the capability to determine the exact confidential or exempt data accessed, acquired, viewed or transmitted by the individual (PR.PT-1)."

The National Institute of Standards and Technology Special Publication 800-14 states, "Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification."

We requested a list of user activity and history logs during the Survey 2 audit period from October 10, 2016, to March 31, 2017, for the NWRDC mainframe/Database 2 (DB2). While we received a list of current and former employees with access to the Student Data Tables from Access Management, neither the NWRDC nor DTI was able to provide an audit trail of user activity. We additionally inquired about user activity and history logs for the Student Data Warehouse. DTI informed us that currently DB2 and the Data Warehouse do not have the ability to track user activity.

Audit logs or trails provide a means to help establish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. With no audit logs to maintain a record of system and user activity and no requirement to periodically review those logs, unauthorized activities can go undetected. That increases the risk of unauthorized access to confidential information and critical data being maliciously or incidentally distorted.

Recommendation

We recommend EIAS develop and implement user access controls for tracking user activity. These policies should include, but not be limited to, establishing and documenting policies for logging of audit records. The logs should support the unique identification of individuals and permit an audit of the logs to trace activities through the system, including the capability to determine the exact confidential or exempt data accessed, acquired, viewed, or transmitted by the individual.

Management Response

Back in 2010, the department started the process of migrating student data collection and processing processes off of the mainframe with the acquisition of SLDS grant. A key goal of SLDS grant was to utilize more current processing methodologies and technical approaches for the source data systems so they can remain compatible with EDW. With this in mind, the department has built a Data Quality preflight system to allow districts to submit and process their student data within an auditable and secured server environment.

Finding 2: EIAS does not have documented policies and procedures for overriding system edits when processing additional or corrective files after the end of a survey period.

F.A.C. Rule 6A-1.0451(4), states, "School districts may submit amendments to student membership survey data in accordance with the following schedule: Survey Period 2 (October) may not be amended after March 31 following the survey."

During FY 2016-2017, the survey week for Survey 2 data was October 10-14, 2016. School districts were required to submit their Survey 2 data by October 28, 2016, and the Statewide Processing Period occurred from October 28, 2016, to November 11, 2016, with a final amendment date of March 31, 2017.

We requested a list of user activity logs during the Survey 2 period for the Student Data Tables on the NWRDC mainframe to determine if overrides occurred after the end of the survey period and whether DTI appropriately authorized the overrides. We additionally requested the department's policies and procedures for determining when files are processed after the final amendment window had closed. According to EIAS, the Office of Funding and Financial Reporting and EIAS jointly determine when it is necessary to allow a district(s) to transmit additional or corrective files for processing beyond the final amendment date. We determined the department does not have documented policies for determining when files can be processed and added to the database after the amendment window has closed, nor is there a formal authorization process for system overrides.

During the scope of the audit, EIAS disclosed that three files from three districts were processed on Monday, April 3, 2017, after the survey-processing period ended. EIAS provided the emails documenting the requests and the justifications for processing the files beyond the final amendment dates. Per the emails, "The decision to process Survey 2 files on Monday, April 3rd, was based on funding issues Brevard's Outward Bound (1020) school was experiencing as a result of Hurricane Matthew. After that decision was made, it was also determined that Broward significantly over-reported FTE and instruction for students at one of its schools, and Alachua had Transportation issues, so those files were processed too."

To allow processing of files after a survey had ended, EIAS modified a table entry. One EIAS staff member made changes to override system edits and allow the acceptance of data into the table, and a second EIAS staff member validated the changes. After these three files were processed, staff updated survey programs to ensure that no other 2016-2017 Survey 2 files would be processed.

Due to the lack of activity logs, we were unable to determine whether EIAS processed additional files after the amendment window had closed. Lack of a formal authorization process, approval process, or policies and procedures for system overrides could lead to the occurrence of unauthorized overrides. The inability to identify responsible individuals to authorize overrides prolongs processing and can effect processing dates for time sensitive data.

Recommendation

We recommend EIAS establish documented policies and procedures for overriding system edits when processing additional or corrective files after the end of a survey period.

Management Response

EIAS will develop policies and procedures for overriding systems edits.

Finding 3: DTI does not have an established Disaster Recovery Plan to restore time sensitive data.

F.A.C. Rule 74-2.006 states, "Each agency shall execute and maintain recovery processes and procedures to ensure timely restoration of systems or assets affected by cybersecurity events. Each agency shall:

(a) Execute a recovery plan during or after an event (RC.RP-1).

(b) Mirror data and software, essential to the continued operation of critical agency functions, to an off-site location or regularly back up a current copy and store at an off-site location.

(c) Develop procedures to prevent loss of data, and ensure that agency data, including unique copies, are backed up.

(d) Document disaster recovery plans that address protection of critical IT resources and provide for the continuation of critical agency functions in the event of a disaster. Plans shall address shared resource systems, which require special consideration, when interdependencies may affect continuity of critical agency functions.

(e) IT disaster recovery plans shall be tested at least annually; results of the annual exercise shall document plan procedures that were successful and specify any modifications required to improve the plan.

The Auditor General evaluated selected IT controls applicable to the department's comprehensive risk assessment process in July 2016. The Auditor General found that, "While the DOE relied on the Northwest Regional Data Center (NWRDC) for disaster recovery (DR) services, the NWRDC DR plan stated that NWRDC staff were only responsible for the recovery of the NWRDC mainframe and the loading of customer data. The NWRDC DR plan further stated that the customer was responsible for performing recovery steps as required once the customer systems were operational; however, the DOE did not have a documented and tested DR plan. Additionally, the DOE had not completed the identification of the IT systems to be designated as critical for priority DR services."

In October 2016, Unisys and Excipio Consulting completed a DR Strategy Assessment for the department. The objectives were to complete a study of the department's current disaster recovery plan for its applications and systems supported by NWRDC. Unisys and Excipio Consulting documented the following findings:

- Lack of a comprehensive, documented DR Plan
- Lack of an application specific DR plan
- Lack of a DR test plan and schedule

We determined the department has not developed a Disaster Recovery Plan, although DTI has completed a Disaster Recovery Project Charter and has begun work with NWRDC to satisfy the department's disaster recovery goals. As of August 14, 2017, the charter had not been signed or approved.

We interviewed DTI staff to determine how frequently the system is backed up for student data and the recovery time for restoration of the student data. The Office of Application and Support stated, "In terms of the School Support Team, when "Initials"[1] are processed for districts on any given day, image copies of all DB2 Tables are made. When Batch processing is ran after the initial processing period, image copies of all DB2 Tables are made on Saturday evening; therefore, image copies of the tables are made, at a minimum, weekly and in the case of when initials run, daily at the application level. In addition, the NWRDC runs Full volume backups daily, Monday – Saturday for the Mainframe DASD environment. It takes approximately 2.5 hours for the backup and it would take about 4-6 hours to restore the data fully."

DTI also stated, "The education data warehouse data is hosted on two Microsoft Windows based SQL servers. These SQL servers and the databases on them are backed up on a nightly basis and on the weekends normally taking about 4.5 hours to complete. Restoration would depend upon the amount of data that would need to be restored."

Both the NWRDC mainframe/DB2, which houses student data tables, and the Student Data Warehouse are mission critical systems and support numerous mission critical processes throughout the department. Lengthy delays in the restoration of the Student Data System could result in data not being available to the public, noncompliance with federal reporting requirements, delays in quality assurance activities conducted by EIAS staff, and in certain circumstances, delays in FTE calculations.

Recommendation

We recommend DTI establish a documented Disaster Recovery Plan to ensure data restoration in a timely manner in the event of a disaster, faulty equipment, etc. These plans should include, but not be limited to, identifying the mission critical IT systems requiring priority DR services, developing a documented and tested DR plan, and identifying recovery steps to perform once customer systems are operational.

Management Response

In the 2014 legislative session, the department was directed to contract with an independent third party consulting firm to complete a study of the department's current disaster recovery plan for its applications and systems supported by the NWRDC. This study was completed by statutory due date of October 2016. The funds for implementing disaster recovery plan were released on July 1, 2017 and the department started implementing the disaster recovery plan.

[1] "Initials" – The original data sets the school districts submit to NWRDC.

Closing Comments

The Office of the Inspector General would like to recognize and acknowledge the Division of Technology and Innovation Office and the Office of Education Information and Accountability Services for their assistance during the course of this audit. Our fieldwork was facilitated by the cooperation and assistance extended by all personnel involved.

To promote accountability, integrity, and efficiency in state government, the OIG completes audits and reviews of agency programs, activities, and functions. Our audit was conducted under the authority of section 20.055, F.S., and in accordance with the International Standards for the Professional Practice of Internal Auditing, published by the Institute of Internal Auditors, and Principles and Standards for Offices of Inspector General, published by the Association of Inspectors General. The audit was conducted by James Russell and Keisha Conyers and supervised by Tiffany Hurst, Audit Director.

Please address inquiries regarding this report to the OIG's Audit Director by telephone at 850-245-0403. Copies of final reports may be viewed and downloaded via the internet at http://www.fldoe.org/ig/auditreports.asp#F. Copies may also be requested by telephone at 850-245-0403, by fax at 850-245-9419, and in person or by mail at the Department of Education, Office of the Inspector General, 325 West Gaines Street, Suite 1201, Tallahassee, FL 32399.