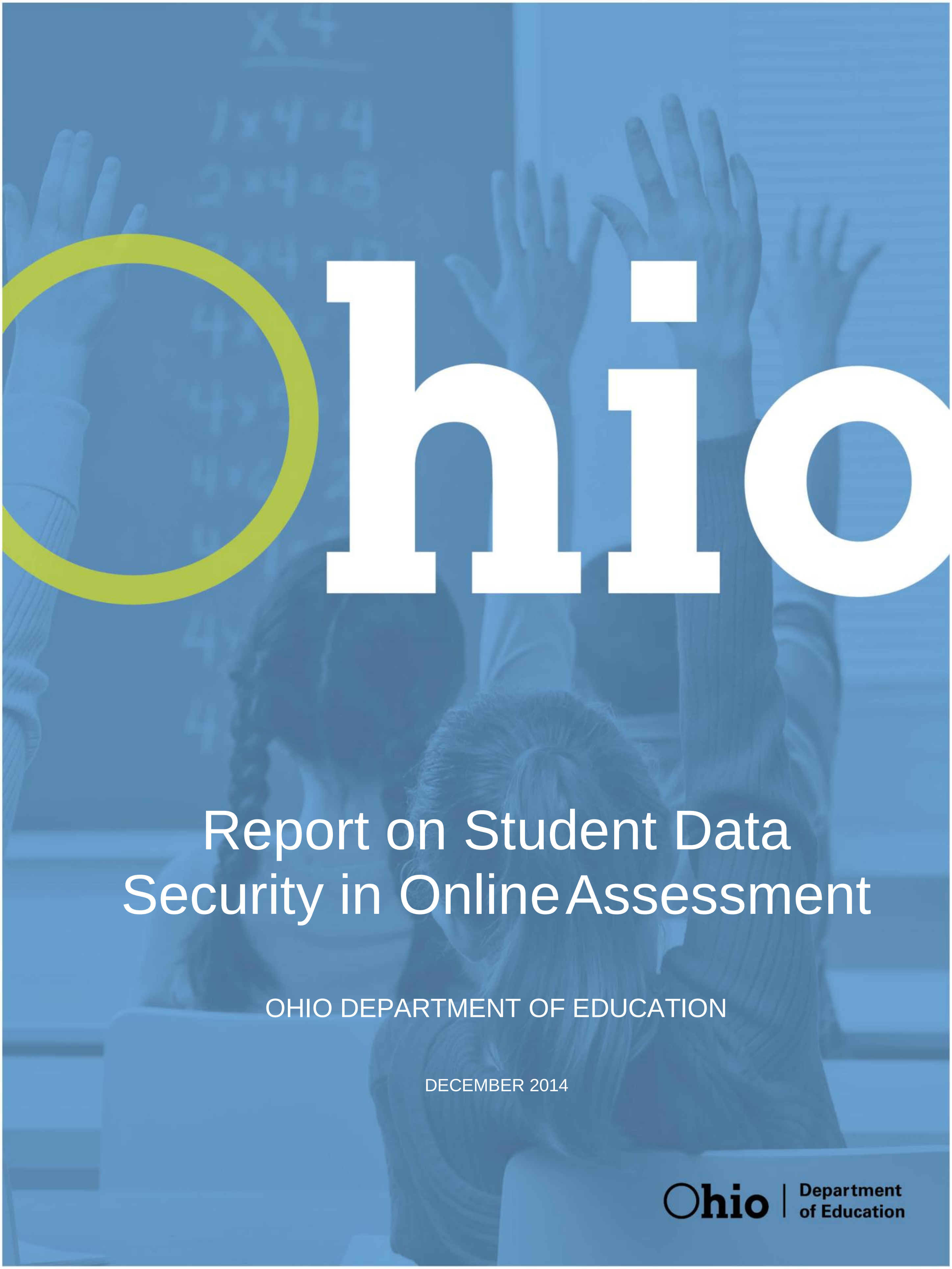

Report on Student Data Security in Online Assessment

OHIO DEPARTMENT OF EDUCATION

DECEMBER 2014

PURPOSE OF REPORT

This report responds to *"Not later than December 31, 2014, the Superintendent of Public Instruction shall submit a report of recommendations to the Governor and the General Assembly, in accordance with section 101.68 of the Revised Code, on the security of student data with regard to the administration of online assessments."*

The Ohio Department of Education defines the scope of this report to be the potential impact of unintentional or unlawful release of personally identifiable student information through online assessments. The scope does not include issues of test security. This is, for the most part, the responsibility of the local school district, which includes issues of archival record retention.

Ohio law, as well as current authorization of the federal Elementary and Secondary Education Act, also known as No Child Left Behind, requires academic performance testing of students.

INTRODUCTION

The focus of this report is on the general assessments for students in grades kindergarten through 12. This assessment includes skills primarily related to English language arts (reading and writing), mathematics, science and social studies. The Ohio Department of Education contracts with assessment vendors to provide a range of services in support of the administration of assessments. This includes, but is not limited to, student registration, assessment login, scoring and reporting (see *Appendix A Test Administration Process*). The department requires that vendors agree to specific terms and conditions in their contracts for services to ensure the protection of student data and to ensure vendors are following state and federal privacy laws (see *Appendix B for Contractual Safeguards*).

Ohio is transitioning from exclusive administration of assessments via paper and pencil to use of online methods for administration of assessments. The department is committed to ensuring protection of student data through both paper and pencil and online methods of assessment administration. There are three main phases of the operation of Ohio testing programs for both paper-pencil and online methods that involve personally identifiable information at the student level. Those phases are: (1) test registration; (2) test administration; and (3) test reporting (see *Appendix A Test Administration Process* for additional detail). As required by state law, this report describes each phase in the following sections followed by a concluding section on the recommendations.

TEST REGISTRATION

Most students are preregistered for testing by the local district. The local district preregisters students by submitting the student's name, statewide student identification number (SSID), the student's date of birth, student demographic data, such as gender and ethnicity, and special student status such as an individualized educational program or migrant status. Students also are associated with a classroom roster during preregistration. The proper assignment of scores to the correct student requires some of these data. Some of these data are necessary for showing the performance of student groupings in required reports. The essence of preregistration is unaffected by whether the student takes an online test or through paper and pencil test booklets. The collection of information is the same by both means. Online assessments do not require districts to submit more student information to the vendor than paper and pencil assessments. Online assessments do not require any additional personally identifiable data than in paper and pencil assessments.

Same-day test registration also is possible and can happen, for example, when a student is new to a district. At present, paper test documents require the input of the student's name, date of birth, ethnicity and identifiers for districts and school buildings using machine-scanned bubbles and written answers. Online testing also will support same-day registration. Additionally, the expectation is that online registration will reduce errors, such as those occurring with the submission of answer documents for scoring.

The transition from paper and pencil to online assessment does not introduce any additional risk of disclosure of student information.

TEST ADMINISTRATION

Using the paper and pencil forms, district personnel affix a pre-ID label to test materials prior to distribution at the testing time. The label includes the student's name, date of birth, ethnicity and gender, as well as a bar code for use by the test vendor. District personnel already have access to this student information, which is necessary to ensure the correct materials are associated with the correct student. This information does not include the SSID of the student or the home address of the student. Online testing also involves a method of identifying the student at the computer terminal through the use of the SSID. District personnel will need to distribute passwords for each student to log in and test.

Using the paper and pencil method, schools collect, pack and ship the student answer documents to the test vendor for processing. As previously described, there is limited personally identifiable information on the ID label or on the bubble section used for same-day registration. Schools have, for the most part, been reliable at returning answer documents because Ohio school accountability measures reward evidence that the student has tested. Online testing will make submittal of student responses paperless and accessible only to the test vendor or the test vendor's subcontractors. Digital data security practices required by the department, outlined in Appendix B Contractual Safeguards, will prevent the interception of these records either for purposes of alteration or disclosure in the same way that online purchases are protected.

Assessment vendors may distribute student-constructed responses (i.e. student written responses, such as short answers, using the Internet for scoring purposes). This already happens with paper and pencil tests. Vendors scan paper and pencil tests and then share in this manner currently to facilitate scoring.

The transition from paper and pencil to online assessment does not introduce any additional risk of disclosure of student information. Use of online assessments reduces the manual processes in paper and pencil assessment and meets the requirements for handling of student data while reducing the risk of human error, including those that could be a security issue.

REPORTING OF TEST RESULTS

The reporting of test results is unaffected by the use of online testing. Regardless of online or paper and pencil administration, the vendor will generate the same reports and distribute them either electronically or in printed format. Printed family reports remain a necessity as well as a prudent practice.

CONCLUSION

In summary, Ohio is transitioning from exclusive administration of assessments via paper and pencil to use of online methods for administration. The department is committed to ensuring protection of student data through both paper and pencil and online methods of assessment administration. The department requires that assessment vendors follow all state and federal laws to protect student data. Online assessment does not provide any new personally identifiable student information to the vendor. The vendor receives the same student data for online assessment as in paper and pencil administration. Use of online assessment reduces manual steps that are associated with student information and data transfer in paper and pencil methods. It helps to eliminate human error and improves data security. Online assessment does not require any new or additional reporting of student data to the federal government. The United States Department of Education or other federal agencies only receive a summary of student data, not individual student-level data. The department, as well as vendors, must comply with all state and federal laws including Ohio Revised Code, Ohio Administrative Code and the Family Educational Rights and Privacy Act.

RECOMMENDATIONS

The department recognizes that districts are responsible for ensuring that the appropriate information security safeguards are in place to protect student data at the local level. It is critical that districts implement the appropriate technical controls and provide education and awareness training to district employees on the procedures and policies related to handling confidential student data. If the appropriate information security policies and procedures are not in place, the district inadvertently could be putting student data at risk in any area of the district that uses or accesses student data. Online assessments are only a small portion of this risk.

The use of technology for online testing is a rapidly changing field. In order to remain current with changing technology, the department will create a committee consisting of all appropriate department offices with the charge to maintain oversight and keep rules and processes up to date. The department will offer periodic meetings to support the implementation of information security best practices at the districts and Information Technology Centers.

Additionally, the department recommends the following:

1. A collaborative effort with the state Office of Information Security and Privacy for the following to provide districts with access to resources, such as, but not limited to, professional development, education and awareness training and best practices models, that will support the adoption of information security best practices and compliance with state and federal privacy laws. Resources shall be included on an education-specific Web page for districts and Ohio's Information Technology Centers.

2. A collaboration with the State Office of Information Technology to explore shared services options that would allow districts to procure the same services and products the state uses to support information security programs.

Appendix A Test Administration Process

		Step 1: Districts register students to take the statewide assessment.	Step 2: Test resources are generated for the students.	Step 3: Tests are administered to the students.	Step 4: Compilation and scoring.	Step 5: Student assessment result data.	Step 5: Districts provide assessment results to the department via EMIS.
Student Data Usage	**Paper-Pencil Administration**	The district uploads student name, SSID, date of birth, school district, grade and other demographics to be transmitted to the testing vendor to build a student profile.	Identification labels are generated and sent to the district to be put on the paper assessment.	Test materials and identification labels are distributed to students. Students take the tests. Each day, materials are collected and then re-distributed the next day. When the test is complete, the materials are collected and shipped to the testing vendor.	The district ships the testing materials back to the school and the test score sheets are scanned, processed and matched against the student data that was uploaded during the registration step. Score results are recorded.	The test results are generated and returned to the district student information system for review and distribution to the families of the students. The results are returned to the district using a secure file transfer method.	Districts upload the testing results from their student information system to the Ohio Department of Education via EMIS reporting. All student data is anonymized and the department only receives the SSID score results. No other personally identifiable information is provided.
	Online Administration		A testing login account is generated for each test taker. The login name and password is provided to the school for each student and the student must reset the password on the first login. When the student logs in, the student should verify the account belongs to him or her.	Students login with their individual IDs to take the tests on PCs or tablets. Once completed with each test portion, the student logs out of the test application and responses are recorded and can be instantly scored.	Student responses are recorded upon finishing the test. The results are automatically matched to the student information based on the test login ID and scores are generated. Test data is instantly available for near real-time quality assurance.		
Student Data Protections	**Paper-Pencil Administration**	All transmissions of student data are required to use a secure file transfer method.	Student identification labels with a limited amount of personally identifiable information and testing materials are shipped to the school district. The district is required to secure the materials and ensure anyone with access to the materials is trained to securely handle them.	The student identification labels have a limited amount of personally identifiable information on them. The district is required to secure the materials and ensure anyone with access to the materials is trained to securely handle them.	Student score sheets with student personally identifiable information are shipped to a secure testing center and stored until processed. There are several manual handling steps which may result in human error.	All transmissions of student data are required to use a secure file transfer method.	All transmissions of student data are required to use a secure file transfer method.
	Online Administration		PII is not required to be shared to manage the login credentials for test takers. Students use their individual logins to take the test.	The testing vendor has minimum system requirements that include a securely configured PC or tablet for test delivery. These requirements include malware protections, access restrictions for students and secure Web browsers. Students are prohibited from sharing login credentials and their usage is monitored during the test. No personally identifiable information is used or shared during the test.	The test is delivered and taken through a secure web application. Responses are returned to the vendors secure data center and scored automatically upon submission		
Security Differences	**Paper-Pencil Administration**	The process is identical for both testing methods	Labels with a limited amount of student data must be stored and handled. Many people are involved in the handling of the data which increases the risk for human error	Labels with a limited amount of student data must be stored and handled daily during the testing. Many people are involved in the handling of the data which increases the risk for human error	Labels with a limited amount of student personally identifiable information are stored at the district until ready to be packaged and shipped to the testing vendor. The sheets are shipped to the test vendor and then stored till they can be processed. There are many manual handling steps in the process.	The process is identical for both testing methods.	The process is identical for both testing methods.
	Online Administration		The list of test login IDs and passwords is handled electronically and the dissemination of information can be secured, controlled, and audited.	No student PII is required to be used or shared during the testing process. Additional quality control steps can be carried out on data during the testing to monitor for testing anomalies	All data is transmitted via secure communication methods. There are no manual handling steps and scoring happens automatically.		

Appendix B Contractual Safeguards

The Ohio Department of Education requires that vendors agree to specific terms and conditions in contracts for services. A contract requires that the vendor comply with federal privacy regulations, and State of Ohio security standards specify how to protect student data. A typical agreement requires that the vendor agree to:

- Comply with federal privacy regulations including FERPA and requires their employees and contractors to comply as well.
- Comply with the State of Ohio security standard, the National Institute of Standards and Technology (NIST) 800-53 Rev. 3 publication and operate at the Moderate Baseline. The moderate baseline specifies how entities implement security controls including items such as:
    - Access Control – How communication access to data and systems is controlled.
    - Awareness and Training – How employees are trained for security policies and procedures.
    - Audit and Accountability – How systems, events and data usage are monitored.
    - Security Assessment – How system security is continually monitored.
    - Incident Response – How the vendor must respond to security events.
    - Maintenance procedures – How systems are maintained to reduce vulnerabilities.
    - Media Protection – How data and the systems that store it are protected.
    - Physical Security – How physical access to data and systems is controlled.
    - Business Continuity and Disaster Recovery – How systems and data are returned to service in the event of an interruption of availability (disaster or outage).
    - Personnel Security – How personnel are screened, hired, and terminated and the security controls pertaining to these events.
    - Risk assessments – How entities manage security vulnerabilities.
    - System and Communications Protection – How systems interact and securely communicate.
    - System and Information Integrity – How systems and data are protected from malware.
- Specific terms for how the vendor may use, store and share data.
- Specific terms for the destruction of data once the contract ends or the data are no longer required to carry out the services in the contract.
- Not disclose or share any data received as a result of the agreement without consent from the department of education.
- Maintain logs of all data requested and transmitted and make the logs available to the department upon request.