FLORIDA DEPARTMENT OF EDUCATION

Student Data Privacy Recommendations

Executive Summary

On September 23, 2013, following the Governor's Education Summit, Governor Rick Scott released an Executive Order announcing a plan for policy improvements discussed during the summit. The executive order addressed state standards assessments, student data security, the school accountability system and teacher evaluations.

The student data security section of the executive order required the Commissioner of Education to (a) immediately conduct a student data security review and issue policies, including internal protocols and operating procedures, for the department, school districts and any assessment provider or other entity with access to student data, in order to protect student information and prevent any unintended use or release of such information, (b) make recommendations regarding any needed rule or legislative change to safeguard the privacy of our students' data by December 31, 2013, and (c) ensure that adequate protections are in place to ensure that no agency, public school, center, institution or any other entity that is part of Florida's education system releases a student's education records without the written consent of the student or parent to any individual, agency, or organization, except as specifically provided by Florida law.

This report contains recommendations for rule or legislative changes needed to enhance the security of students' data in response to the Executive Order.

Background

Department information systems are managed primarily by the department's Division of Technology Information Services (DTIS). Multiple offices and systems in the department receive and store student data, including the Division of Accountability, Research and Measurement (ARM) and the Office of Student Financial Assistance (OSFA).

Florida Statutes charge the department, school districts and postsecondary institutions with specific requirements for collection, management, reporting and security of educational data, including student data. The department collects and validates student data from educational entities, such as school districts and postsecondary institutions, through a series of steps involving technologies and processes at the Northwest Regional Data Center (NWRDC) and the Southwood Shared Resource Center (SSRC).

K-12 student data is primarily housed at these two data centers under service level agreements (SLAs) between the department and the data centers. Under the SLAs, the department retains full

data ownership. In regard to security of data, the SLAs note that the data centers presently house data that are sensitive and confidential under state and federal laws. The SLAs also require the department to disclose the existence of all sensitive data that may fall under any state or federal guidelines which would require the data centers to provide additional security measures.

Requirements for a number of projects, such as those required to implement education programs under Florida Statutes and those associated with Race to the Top (RTTT) initiatives, have given rise to increased systems and applications development over the last few years. The addition of many new systems with user needs for data access, such as Local Instructional Improvement Systems (LIIS) for Florida's school districts, requires the department to implement comprehensive security controls.

Controlling Laws

Federal Regulations

The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g and implementing regulations in title 34 CFR Part 99, which is incorporated by reference into Florida law in section 1002.22, Florida Statutes, concerns privacy of student information and applies to all schools that receive U.S. Department of Education program funds. Parents or eligible students (students to whom rights have transferred upon reaching age 18 or upon attending a postsecondary educational institution) have the right to inspect and review the student's educational records maintained by the student's school. Parents or eligible students also have the right to contest the content of educational records and the right to a formal hearing if the school decides not to amend the record. If, after the hearing, the school decides not to amend the records, the parent or eligible student may enter into the record a statement regarding his or her view about the contested information.

FERPA allows school officials to release student information without parental or student consent in certain circumstances including the following:

- to other school officials within the institution or local education agency determined to have a legitimate educational interest;
- to schools to which a student is transferring;
- for official audits or evaluations;
- when related to financial aid;
- when required by certain studies on or on behalf of the school;
- for accrediting organizations;
- when court-ordered;
- when required by health or safety emergencies; or

- to state and local authorities within a juvenile justice system.

Schools may also disclose "directory" information (e.g. names, addresses, telephone numbers, birth dates, honors and awards, and dates of attendance) without consent, although schools must inform parents or eligible students of information it has designated as directory information and must provide them an opportunity for opting out of directory information disclosure. Once a parent or student "opts out" of inclusion in a school district's directories, that selection does not need to be repeated unless and until the student enrolls in a different school district.

State Statutes and Rules

Section 282.318, Florida Statutes, and Chapter 71A-1, Florida Administrative Code, require the department to develop, document, implement and maintain an agency-wide information security program that is administered by an Information Security Manager (ISM). The purpose of the program is to safeguard the confidentiality, integrity and availability of department data and information technology resources. The rule also defines minimum standards as well as minimum management, operational and technical security controls to be used by agency information security programs. Both the statute and the rule require the Agency for Enterprise Information Technology (AEIT) to provide oversight for executive branch agencies; however, AEIT was decommissioned in 2012 after no longer receiving a legislative budget appropriation.

Section 282.318(4)(2)(c) and Rule 71A-1.020(3) require agencies to conduct a comprehensive risk analysis every three years to determine security threats to the agency's data, information, and information technology resources. In 2011, in coordination with AEIT, the department's information security staff conducted a tri-annual risk assessment. A summary of the results of the most recent assessment are described later in this report.

Section 1008.385(2), Florida Statutes, requires the Commissioner of Education to develop and implement an integrated information system for educational management. The system must be designed to collect, via electronic transfer, all student and school performance data required to ascertain the degree to which schools and school districts are meeting state performance standards, and must be capable of producing data for a comprehensive annual report on school and district performance. Each district school system that operates a unique management information system shall assure that compatibility exists between its unique system and the district component of the state system, so that all data required as input to the state system is made available via electronic transfer and in the appropriate input format.

Rule 6A-1.0014, Florida Administrative Code, requires the department and each school district to develop and implement an automated information system component which is part of and compatible with the statewide comprehensive management system. Each component shall

include procedures for the security, privacy and retention of automated records, in accordance with FERPA, the implementing regulations issued pursuant thereto, and Section 1002.22.

Rule 6A-1.0014(2) requires the department to publish information database requirements manuals for the automated student, staff and finance information systems. These publications include the department's procedures for the security, privacy and retention of school district student records collected and maintained at the state level. The procedures outlined for student records in the publication *DOE Information Data Base Requirements: Volume I – Automated Student Information System*, dated July 1, 2013, state the following:

- Individual, personally identifiable student records collected and maintained by the department shall be accessible only to authorized state education officials for the purposes of auditing, monitoring and evaluation of state and federal education programs, or for the completing of federal or state mandated activities requiring access to such records as prescribed by FERPA, the implementing regulations issued pursuant to FERPA, and section 1002.22.
- The department shall not disclose personally identifiable, individual student records to any person, institution, agency or organization except as authorized by FERPA, the implementing regulations issued pursuant to FERPA, and section 1002.22.
- Personally identifiable, individual student records shall be utilized by the department to prepare and publish only aggregate reports and analyses, and such personally identifiable, individual student records shall be destroyed in accordance with the records retention procedure prescribed below.
- Access to individual student records will be stringently controlled through technical security conventions and procedures established by Northwest Regional Data Center. Appropriate computer passwords and Logon IDs shall be assigned to users in order to establish each user's data access authority only to the records or data elements required to complete federal or state mandated activities.
- Individual, personally identifiable student records shall be destroyed according to a records retention schedule established by the Department of State, Division of Library and Information Services, Records Management Program, consistent with the requirements of section 257.36, Florida Statutes. Personally identifiable student records shall be maintained for five years or until applicable federal or state audit functions have been completed, at which time all such records shall be destroyed except for those required for the evaluation of state or federal education programs. Personally identifiable, individual student records maintained for the evaluation of state or federal education programs shall be destroyed when no longer required.

Department Security Initiatives

Department Information Systems

The department's Education Information and Accountability Services (EIAS), Community College and Technical Center Management Information System (CCTCMIS) and the Educational Data Systems (EDS) sections fully utilize the security capabilities provided by NWRDC and use all of the extensive security features found in NWRDC's IBM DB2 (DB2) environment. The DB2 security features include facilities for restricting the types of data access granted to a user (select access, update access, add access, and delete access). Access can also be limited to specified data elements within a file or denied entirely.

Individual, personally identifiable student records collected and maintained by the department may be accessed only by authorized individuals as prescribed by FERPA, the implementing regulations issued pursuant to FERPA, and section 1002.22. EIAS, CCTCMIS and EDS are prohibited from disclosing such records to any person not authorized by these laws and regulations.

Access to the databases themselves is restricted to properly authorized individuals or school districts by user ID and password. School districts are limited to access to their own data. DB2 does not allow user access to any data table unless the creator of the table grants permission to that user's ID. The EIAS bureau chief controls and grants all access to the student and staff information databases according to the department's security procedures through the DTIS. The CCTCMIS bureau chief grants access to the Florida College System and Workforce Development Information System databases in the same manner.

The department is developing an implementation-ready unique personal identifier called the Florida Education Identifier (FLEID) that will improve data security and accuracy. Key characteristics of the FLEID system include PK-20 (system-wide) use; improved data matching processes; establishment of an especially secure vault containing all personally identifiable data; and inclusion of the tools necessary to assign, manage and edit ID assignments between the department, districts and institutions in a more secure and consistent manner.

Information Systems Security Governance

The descriptive information in this section is taken primarily from the risk assessment of 2011 conducted with Agency for Enterprise Information Technology and the department's actions taken in response to that report.

Information Security Program

Section 282.318, Florida Statutes, and Chapter 71-A, Florida Administrative Code, require the department to establish an agency information security program. The department has developed an information security program and has appointed an ISM to administer the program.

Strategic and Operational Information Security Plans

In July 2013, in accordance with Rule 71A-1.003(3) and section 282.318, the department's information security staff prepared a strategic information security plan and associated operational information security plan. Both plans have been developed but do not fully describe some required components.

Data Classification

Rule 71A-1.020 requires agencies to categorize information technology resources according to the process outlined in Federal Information Processing Standards (FIPS) Publication 199. The strategic and operational information security plans note that a data classification process based upon FIPS 199 is planned to be implemented for fiscal years 2013–14, 2014–15, and 2015–16. The department's internal operating procedures note that protection of data is the responsibility of department management and delegated data owners, and a draft data classification policy describes procedures which require agency data owners to classify information as confidential or public and to be responsible for authorizing access to information.

Monitoring, Cataloguing, and Locating Data

Beginning in June 2013, the department entered into a series of contracts with Dell SecureWorks (SecureWorks) in which SecureWorks would provide information security consulting, monitoring, and assessment services, the duration of which range from one year to three years Department staff reported that the use of SecureWorks monitoring services has aided them in becoming more aware of potential security issues. The department continues to use this tool and processes learned to catalogue and organize current projects in a more efficient and secure manner.

Email

Rules 71A-1.006 and 1.019 require the department to encrypt information exempt from public records disclosure and "confidential and exempt" information sent by email. The current strategic and operational information security plans indicate that a secure file transfer solution is partially in place to "meet business needs that email cannot address" and is planned to continue during 2013–14, 2014–15, and 2015–16. The department currently uses Cisco Ironport Encryption software which works in conjunction with users' Microsoft Outlook email systems for sending encrypted email messages. Also, the document "*Sending Encrypted Email Attachments using AxCrypt*," available to users on the department's intranet, explains how to encrypt email attachments using AxCrypt shareware.

Mobile Devices
Rule 71A-1.006 and 1.011 require that mobile computing devices with exempt or confidential and exempt department information are encrypted, and that mobile storage devices with exempt or confidential and exempt department information have encryption technology enabled. The current strategic and operational information security plans indicate that purchasing, installation, configuration and administration of a mobile device management solution to improve wireless security and mobile security is partially in place and planned for further implementation in fiscal years 2013–14, 2014–15, and 2015–16. The document "*Sending an Encrypted CD/DVD Using TrueCrypt,*" available on the department's intranet, explains how to encrypt CDs and DVDs using TrueCrypt shareware. Although both AxCrypt and TrueCrypt are shareware products, they meet the Advanced Encryption Standard (AES) algorithm standard. AES is an algorithm included in the definition of "strong cryptography" in Rule 71A-1.002.

Data Transmission
Rule 71A-1.006 requires the department to encrypt electronic transmission of exempt and confidential and exempt information when the transport medium, or network, is not owned or managed by the department. The current strategic and operational information security plans indicate that to improve virtual private network (VPN) and wireless security, the purchasing, installation, configuration and administration of a mobile device management solution is planned for fiscal years 2013–14, 2014–15, and 2015–16.

Rule 71A-1.022 requires wireless transmission of department data to be implemented using strong cryptography for authentication and transmission. The current strategic and operational information security indicate that purchasing, installation, configuration, and administration of a mobile device management solution to improve wireless security and mobile security is partially in place and planned for planned for fiscal years 2013–14, 2014–15, and 2015–16.

Security Requirements for Non-Agency Entities
Rule 71A-1.005 requires the department to develop procedures to ensure that security requirements are specified throughout the procurement process for information technology services, to ensure contracts and agreements include language whereby the contractor/partner agrees to comply with agency information technology security policies, and to ensure that non-agency entities execute a network connection agreement that will ensure compliance with agency security policies prior to allowing non-agency entities to connect to the agency internal network. The department's 2011 risk assessment noted that at the time the department's Technical Advisory Group served as an advisory group for oversight and integration of technology solutions, along with Change Management and NWRDC. Additionally, the department used a system of secure VPNs for all external network connectivity. DTIS staff indicated there is not

currently a centralized process for ensuring SLAs and contracts involving the use of departmental information security resources or exchange of sensitive data are compliant with security requirements.

School District Activities

Section 1008.385, Florida Statutes, requires school districts to maintain a management information system to aid in identifying and meeting the educational needs of students and the public. The system must be structured to meet the specific management needs of the district and to align the budget adopted by the district school board with the plan the board has also adopted. Each school district management information system must assure compatibility exists between its unique system and the district component of the state system, so that all data required as input to the state system are made available via electronic transfer and in the appropriate input format.

Rule 6A-1.0014(1), Florida Administrative Code, requires each school district and the department to develop and implement an automated information system component, which shall be part of, and compatible with, the statewide comprehensive management information system. Each information system component must contain automated student, staff and finance information systems and must include procedures for the security, privacy and retention of automated records. The procedures for the security, privacy and retention of automated student records shall be in accordance with the requirements of FERPA, the implementing regulations issued pursuant to FERPA, and section 1002.22, F.S.

IT Security Reviews

SecureWorks Assessment Results

SecureWorks conducted an assessment of the department's information security program in October 2013. The goal of the assessment was to determine the current state of the department's information security program as compared to regulatory guidance and industry accepted standards. As a result of the assessment, and in regard to governance, data classification and exchange of sensitive data, SecureWorks noted the following findings based on their review process and indicators:

- Many policies, practices and technical controls within the scope of the assessment only partially met best-practice standards. No formal IT steering committee existed. A lack of IT governance limits the department from establishing and enforcing strong information security policies.

- No formal policies for data classification had been approved by senior management, although an informal draft data classification policy did exist that adequately outlined the department's data types.
- No formal encryption policy or procedures existed. Encryption was not being used on mobile devices such as laptops. No formal policy existed requiring the use of encryption for sensitive information sent via email.
- No detailed process for the management of third party remote access to department networks existed.
- No formally documented requirement to review security requirements for new systems existed. New technology and applications were not centrally managed and governed by IT but instead by disparate groups using grant money for projects. However, there was an informal process in place requiring the review of security requirements when acquiring significant system components.

In light of the above, SecureWorks made the following recommendations:

- An IT steering committee process should be developed, documented and implemented, with committee members representing all major departments.
- Senior management should review and formally approve the draft data classification policy.
- An encryption policy and procedures should be established to ensure that encryption is used appropriately and consistently throughout the department, and should include the use of encryption, how sensitive information should be protected by encryption, key management, recovery methods, roles and responsibilities, a requirement for only approved strong encryption methods, and internal and external encryption methods.
- A third-party remote access control process should be developed, documented and implemented, and should include approved methods for remote third party to ensure that no improper access is granted to vendors or third parties.
- All applicable security and business requirements should be identified and documented, and a review of requirements should be formally integrated into the system acquisition process (via additional steps in a project plan or integrated into the RFP process).

Auditor General Operational Audit

An independent audit on the department's compliance with applicable statutes and rules related to information security is currently being conducted by the Florida Auditor General. Although no results have been released for this audit, the department stands ready to implement or enhance its policies and procedures based on the Auditor General's recommendations.

Legislative Recommendations

The department recommends the following changes to Section 1002.22, F.S.:

- Requiring that notice be given annually by school districts to parents and students of their rights with respect to education records.
- Establishing limitations on the collection of information for school districts, schools and other educational organizations or entities that are part of Florida's education system, to include the prohibition of the collection, obtainment, or retaining of biometric information; political affiliation; voting history; religious affiliation for students, parents, or siblings of students; health information including health care plans; and correspondence from community agencies or private professionals.
- Establishing limitations on the disclosure of confidential and exempt student records for school districts, schools and other educational organizations or entities that are part of Florida's education system, to include the prohibition of providing education records made confidential and exempt except when authorized by state statute, federal law, or in response to a lawfully issued subpoena or court order.
- Requiring that governing boards of agencies or institutions may only designate directory information in accordance with FERPA at a regularly scheduled meeting that must consider whether disclosure of such information would put students at risk.
- Clarifying that a parent or student who has received injunctive relief upon brining an action in circuit court to enforce his or her rights under these policies by injunction may be awarded attorney's fees and court costs.

The department further recommends that the legislature consider enacting legislation that requires, and provides resources for, the creation of a data inventory that identifies and defines individual student data fields that are currently being captured and retained by the department. Any student data required to be reported by federal or state mandates should be noted. Any student data captured by the department that is not mandated by rule or statute should be identified and consideration should be given to ceasing the collection of those data elements. The department should not capture or retain any individual student data without a definite purpose or reason based on current state or federal laws and reporting requirements.

To ensure the maintenance of confidentiality of the student records maintained in the management information system, the assignment of a student identifier within state and local systems should be established to help to protect the confidentiality of individual student records. The student identifier should be computer-generated and contain no embedded meaning.

The department must ensure that technologies being utilized throughout the agency follow industry standard best practices. These practices shall include: the alignment of all technology

initiatives to the strategic mission, vision and goals of the agency; proper monitoring and management of each initiative; assurance that each initiative delivers the benefit as promised; assurance that technology resources are managed efficiently; measurements for the risks associated with each initiative; and measurements for the performance of each initiative. To achieve this, the department should periodically submit to the State Board of Education a report showing the agency's key initiatives with a status of each initiative and how these practices are being followed for each of the initiatives.

A report should also be provided to the State Board of Education at the beginning of each fiscal year providing a status update on security reviews and any new procedures or processes implemented in the area of data security.

The department has increased its security posture by utilizing RTTT funding to employ the services of SecureWorks. This has included extensive log monitoring and analysis of the entire RTTT environment, vulnerability scanning, application scanning, incident response services, and an information security assessment. This has effectively created a security umbrella for the RTTT IT environment; however, most of the department's IT infrastructure lies outside this security umbrella. To address this need, the department has submitted a Legislative Budget Request (LBR) for continued funding to maintain the existing services and to expand these services to include all department information technology systems. The current security umbrella infrastructure is essential to ensuring the privacy of student data from internet-based vulnerabilities. Currently, because of these services, the department has been able to improve its security posture by stopping discovered attacks before system compromise, strengthening security on vulnerable systems, and implementing tighter security controls on business processes. The continuing success of this security umbrella hinges on sufficient funds being allocated to the department to continue providing state-of-the-art security measures for the department's student data.

Department Recommendations

The information security review for this report focused on general information security controls, and specifically governance, data classification, and exchange of confidential data, as well as issues affecting student data security. The following are recommended actions the department could take that do not require additional legislation:

Governance

1. The department should increase efforts to improve information security governance. A formal information security charter should be developed, with defined organizational and individual roles and responsibilities. An information systems steering committee should

be established. It is recommended that such a committee be composed of diverse membership and include representation from executive management, business units, IT and information security, human resources, legal, risk management, audit, operations and communications. Goals of the committee may focus on aligning the security program with organizational objectives and promoting good security practices and policy compliance.

2. The department should increase efforts to review, modify as necessary, and formally approve proposed information security policies and procedures.
3. The department should review and revise the information security strategic and operational plans as necessary to ensure that all required components are included.
4. The department should formalize data security language to be included in, and a process for DTIS to review, contracts, grants and procurements.

Data Classification

1. In accordance with Rule 71A-1.020, F.A.C., the department should categorize information technology resources according to the Federal Information Processing Standards (FIPS) Publication 199. This process estimates the magnitude of harm that would result from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource – low-impact, moderate-impact, or high-impact relative to the security objectives of confidentiality, integrity, and availability.
2. The department should review and approve, with modifications if necessary, its proposed data classification policy, and include a reference to implementation of a FIPS 199 process as required in 71A-1.020, F.A.C.

Exchange of Sensitive Data

1. The department should review and approve, with modifications if necessary, the proposed policies related to exchange of confidential data, including policies for mobile device use, wireless and remote access, email, and cloud storage and transfers.
2. The department should maintain a focus on ensuring that the encryption standards in Chapter 71A-1, Florida Administrative Code, are implemented.
3. The department should review practices and procedures for SLA and contract management to ensure that contracts or agreements involving the exchange of sensitive data are compliant with security requirements.

Additional Issues Related to Student Data Security

1. The department should standardize masking procedures throughout the department to ensure that confidentiality is maintained in all public reporting of educational records.
2. The department should conduct annual security training for department personnel whom are responsible for collecting or using personally identifiable student information.

3. The department should consider establishing a student data privacy and security task force for continuous alignment of student data privacy and security practices. The task force could coordinate communications for best practices with nation-wide and privacy resource entities such as the Privacy Technical Assistance Center (PTAC) and the Data Quality Campaign (DQC).

District Recommendations

To ensure the privacy and security of student data at the district level, each school district should be required to implement security policies and practices similar to those mentioned in this report that the department is required to implement.

School districts should ensure that any entity accessing personally identifiable information for federal or state program purposes through authentication and authorization protocols maintained by the department must remove such access when it is no longer needed for the purpose specified in the request for access. Each district must provide written notice to the department for access removal within twenty-four hours of a status change.

Districts' internal policies and procedures that ensure compliance with FERPA and other relevant privacy laws to protect student data should be audited on a periodic basis.

Any recommendations required for school districts should also be applied to Regional Educational Consortia, which process student data on behalf of member school districts.