Testimony before the
House Education Committee on Data Security

DELIVERED BY
Drew Lane, Executive Director of Information and Communication Technologies
Shawnee Mission School District

February 12, 2015

Chairman Highland and Members of the House Education Committee, thank you for the opportunity to appear before you and to present information on behalf of the Shawnee Mission School District regarding data security.

My name is Drew Lane. I am the Executive Director of Information and Communication Technologies for the Shawnee Mission School District. In my role with the school district, I am charged with the management of the people and systems responsible for data collection, storage, and transmission. It is my responsibility and that of the Shawnee Mission Board of Education to maintain a strong security stance for the school district.

The House Education Committee has received wide-ranging testimony about problems and issues perceived by some to exist with student data and the privacy and security of technology systems containing those data. I will address those concerns.

In the performance of its regular business activities, the Shawnee Mission School District collects, stores, and transmits sensitive student data as required by the state and federal government. The board of education, administrators, and staff, many of whom are also parents and taxpayers, take these issues very seriously. We do not sell student data. We retain medical data on students only as necessary related to the safety, security, and well-being of students. This necessary data includes immunization records, known allergies, and/or other data that parents impart to us. Data security is a foundational component of all collection, storage, and transmission activities during the lifecycle of the data, and the school district has processes in place to protect this sensitive data.

The district complies with all federal and state laws pertaining to data collection, storage, and transmission such as the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), and more recently KSA 72-6215 through 6223 (Student Data Privacy Act), which is also known as Senate Bill 367 that passed in 2014.

To ensure that the district follows best practice for collection, storage, and transmission of data, the Shawnee Mission School District adheres to industry standards such as those described in the National Institute of Standards and Technology (NIST) Special 800 Publications and the Payment Card Industry (PCI) Data Security Standard (DSS).

To maintain a strong security stance and meet obligations as they pertain to data collection, storage, and transmission, district security controls are in place.

Security Controls

Both physical and logical security controls must be in place and are key to any strong security stance. Controls are applied in layers and at critical junctions across the many networks, systems, and cloud-based services in use.

In terms of physical security, the Shawnee Mission School District utilizes card-reader controls to limit physical access to sensitive data center areas. Access is limited to technology personnel who have a valid, work-related need. Valid, work related need is determined with input from district security personnel and the appropriate supervisor or administrator in consult with the executive manager of information and communication technologies.

Logical controls must also be in place to provide an additional measure of protection. One important control is account management. The use of strong, complex passwords, account lockouts, and varying lockout durations represent solid approaches to keeping sensitive data secured behind role-based, credentialed access. This also serves to limit access to sensitive data to only those persons with a valid, work-related need, which uses the procedure I previously defined.

Securing networks is another important component of the district's strong security stance. The district requires both device and user authentication to access district networks. This provides an additional verification of restricted access to sensitive data. Remote access is limited as well and requires virtual private network (VPN) access credentials. Enterprise-class firewalls, routers, and switches are used to help harden networks against unauthorized access.

Additional measures provide further strengthening of the security of the district's information systems. Two-factor authentication; enterprise-class anti-virus, malware detection, and mitigation software; regular patch management; and intrusion detection/intrusion prevention systems are in place in the Shawnee Mission School District. School districts are legally bound to maintain software systems and data protection measures. The Shawnee Mission School District complies with these requirements updating software regularly to guard against any breach of data.

Secured transmission methods are employed including the use of Secure Socket Layer (SSL) and Transport Layer Security (TLS) for all public-facing access to data that is of a sensitive nature. The district requires identification verification of personnel and patrons requesting access to data. Sensitive, personally identifiable information (PII) is encrypted prior to transmission. The district adheres to PCI DSS to keep financial transactions conducted in the district secure and safe. District uploads to the state-required KIDS system are conducted across secured and encrypted transmissions. The district also

requires employees that need additional access to sensitive data to sign a document acknowledging their responsibility for data security. For example, a technology staff member requires access to information about students who qualify for free and reduced lunch to ensure data is flowing correctly and accurately within district systems.

Audit review, analysis, and reporting are also core components of the district's security protocol. Designated personnel are responsible for monitoring system records for indications of unusual or inappropriate activity. Those employees are also tasked with investigating suspicious activity or suspected violations. Additionally, those individuals report their findings to appropriate officials and take necessary actions to mitigate any issues. To know the district's vulnerabilities, third-party, external vendors are engaged to perform penetration tests and vulnerability scans.

Two other key components for which the district has a responsibility are off-premise data security and management of data that has reached end-of-life. For off-premise devices, the district has systems that allow personnel to remotely erase devices that may have been compromised, stolen, or lost. When data reaches end-of-life, the district sanitizes all digital media to Department of Defense (DoD) standards. Non-digital media is cross-cut shredded and destroyed before disposal.

While security controls are critical to a comprehensive security stance, keeping people informed and instilling a security awareness mindset are also crucial.

Training and Informing Personnel

The district recognizes the importance of engaging people to educate them about best practice and helping them develop and maintain a security-conscious mindset. The Shawnee Mission School District addresses this human component by regularly reviewing, developing, and adapting the district's security awareness program so that it meets changing needs. The district employs professionals with industry certifications such as the Certified Information Systems Security Professional (CISSP) to help navigate the ever-changing data security landscape and to keep other personnel aware of new or evolving threats, processes, and procedures. District personnel regularly meet with security vendors to review, test, and discover new security technologies. The district's security stance also emphasizes the importance of being discerning when approached about sensitive data to avoid becoming a victim of social engineering.

The district also recognizes a responsibility for communicating issues related to data security with parents and patrons.

Communicating with Parents and Patrons

Parents and patrons should be aware of the information the district collects, stores, and transmits. They should also be aware of the district's obligation and commitment to keep sensitive data private and confidential. The Shawnee Mission School District is committed

to helping parents and patrons understand the district's obligations and responsibilities. Annually, the district places public notices in the Kansas City Star, the district's paper of record, about the district's compliance with the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA). Updated notifications are available via the district's web page and a communications infrastructure is in place to relay information across the district should a breach of some kind occur. The district has also ' communicated with parents this year regarding technology and technology-related issues. Communication has included information to assist parents in developing an awareness regarding safe and responsible use of technology and encouraging digital citizenship as it relates to the district's digital learning initiative. The district continues to inform parents of the importance of maintaining limited access to student information as evidenced in the notices for accessing the Family Access portion of the district's Skyward student information management system.

As technology continues to change and data continues to be an important concern, the district will continue to engage and communicate with parents and patrons on this topic.

In closing, I would like to again thank the committee for the opportunity to present information regarding data security. To summarize our key points, the Shawnee Mission School District:

1. Does collect, store, and transmit sensitive student and personnel data as required by the state and federal government.
2. Recognizes and takes seriously the obligations that go along with collecting, storing, and transmitting sensitive data.
3. Adheres to all applicable federal and state statutes.
4. Follows industry best practice for implementing security controls to keep sensitive data secure and addresses with staff the importance of having a security-conscious mindset.
5. Engages in communicating district obligations and responsibilities with parents and patrons.

Thank you for your time, and I will stand for questions.