LPSD Technology Board Report

March 2026 - Sam Rigby

E-Rate FY27

The competitive bidding process for FY27 internet service at schools has concluded. We received five proposals from GCI, ACS, Microcom, SVG, and FiberFed. All proposals were evaluated and scored against a pre-determined evaluation matrix. Microcom received the highest score and will be awarded the contract for all locations. After factoring in the E-Rate discounts, LPSD's actual out-of-pocket cost will be approximately $47,000 for the year. We are only signing a one-year contract, but have the option to renew for multiple years without needing to go out to bid again.

Embrace IEP Transition

For the past several years, the cost of the PowerSchool SPED records software was subsidized by AK DEED. They recently announced a transition to a new vendor, Embrace, for SPED records. LPSD had the option to continue paying the full price for PowerSchool SPED or switch to the new platform, and we chose to move to Embrace. This was a significant project, requiring our IT and student data teams to migrate all active IEP records, set up secure access, and establish automatic data synchronization between our student information system and Embrace. I want to extend a big thank you to Cassie and Nate for leading the student data portion of this transition.

State Testing Tech Prep

With the state testing windows rapidly approaching, we have prioritized preparing student devices with the two testing applications: NWEA State Solutions and DRC Insight. We experienced minimal technical disruptions during testing last year, and we anticipate continued technical success this year.

Cybersecurity

Over the past several weeks, our security monitoring system detected two coordinated cyberattack campaigns targeting LPSD servers. These attacks, known as "brute-force" attacks, use automated tools to guess login credentials repeatedly in an attempt to gain unauthorized access to district systems. We flagged over 700 security alerts across a three-day period, with attackers making 127 unauthorized login attempts from 15 different IP addresses. A second campaign in mid-March generated 25 additional high-severity alerts, with one source alone probing our systems every one to two hours.

In both cases, no accounts were compromised and no data was accessed. Our team identified the attacking IP addresses and added them to a firewall blocklist, preventing those sources from reaching district systems entirely.

We are seeing a broader industry trend of AI-assisted attack tools that probe for vulnerabilities more intelligently and persistently than older methods. This makes active security monitoring increasingly important, and we are continuing to tighten controls around remote access and sensitive data to stay ahead of these threats.