MISSISSIPPI

Follow-up Report

Cybersecurity in School Districts

June 2022

SHAD WHITE
State Auditor

Jessica D. McKenzie
Director, *Government Accountability Division*

STATE OF MISSISSIPPI
OFFICE OF THE STATE AUDITOR
Shad White
STATE AUDITOR

May 24, 2022

Auditor's Letter

In a report called the *Children's Internet Protection Act (CIPA) Compliance Review*, issued in 2017, the Office of the State Auditor (OSA) identified explicit material on school computers. The Office issued four recommendations to prevent this in the future, as well as additional guidelines released in a document entitled *Cybersecurity Best Practices*. With this latest report issued today, OSA's Government Accountability Division is following up on the 2017 recommendations to ensure corrective action has been taken.

Despite the efforts of many school districts, OSA analysts determined the risks associated with the original findings still exist. One of the biggest issues is what happens when students take computers home. Only about one out of every five school districts ensures that their explicit materials policies are enforced when computers are taken off campus. Fewer than half of districts have technology that actively alerts administrators when someone uses a school computer for an inappropriate purpose. This sort of technology, which is currently used in districts like Petal School District, is available for use.

The danger of computers accessing explicit content has been magnified by the large amount of stimulus spending on technology in public schools in the last two years. I hope our report is useful to policymakers and district officials as they consider how to protect children in the wake of that wave of spending.

The *Highlights* page in this report provides background and summary information about the original 2017 review. Following the *Highlights* page is an update on the implementation of the 2017 report's recommendations. I would like to express my sincere appreciation to all the school districts who participated in this review. For any questions regarding these findings, please contact the Auditor's office at 601-576-2800.

Mississippi Office of the State Auditor

Shad White, State Auditor

Highlights from the Original Report

In 2017, the Office of the State Auditor conducted a review of nine school districts and found that students were able to access pornography or other explicit material. OSA conducted the review of school districts' compliance with the Children's Internet Protection Act (CIPA) for the 2016-2017 school year.[1] The purpose of the review was to test the reliability of the security controls districts have in place and the filters, if any, installed on publicly owned devices that are issued to and utilized by students across the state.

OSA's objective was to ensure districts were protecting students from harmful and/or inappropriate material while accessing the internet with school issued devices. Under the CIPA requirements, school districts must have an Internet Safety Policy (ISP), Technology Protection Measures (TPM), and provide public notices and hearings or meetings to address the proposed TPM and the ISP. TPM is a specific technology that blocks and filters internet access to material that is considered obscene and/or harmful to minors.[2]

OSA tested eighteen (18) schools within nine (9) randomly selected school districts to ensure security controls of online activities were effective. During this process, 150 random devices were analyzed. Of the 150 devices tested, 30 (20%) of the devices showed evidence that students were able to access explicit material on school issued devices.

Evidence also indicated that the districts' filtering systems were ineffective when filtering inappropriate material. The nine (9) districts reviewed did not enforce their Internet Safety Policies or Acceptable Use Policies (AUP) by ensuring the TPMs were effective while students had access to the internet. In addition, of the nine (9) districts reviewed, one (1) school district did not maintain TPM filtering when students were off school grounds.

OSA also measured districts' compliance with having a policy to monitor the online activities of minors. It was determined that all nine (9) districts had a variety of written policies and technologies that block and filter devices issued to students. However, OSA discovered inappropriate material on students' devices. It appeared that districts were not completely adhering to their own policies. OSA offered four recommendations directed at school districts in response to these findings and issued the *Cybersecurity Best Practices* document for school districts and their information technology staff.

[1] MS Code § 7-7-211 through § 7-7-215, gives OSA the authority to audit publicly owned property of the state of Mississippi including computers and/or laptops issued to students in Mississippi's public schools primarily through the One-to-One initiative.
[2] The Federal Regulation code 47 CFR §54.520(c)(2)(i) states "...The Internet safety policy and enforced pursuant to 47 U.S.C. 254(h) must include a technology protection measure that protects against internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors...."

Follow-Up Status: *Most School Districts are not Enforcing the Policies they Adopted to Protect Students*

OSA conducted a follow-up review to evaluate implementation of select recommendations. Each school district surveyed, a total of 136, was required to submit evidence to support their responses when applicable.[3] The results show that cybersecurity in school districts continues to be a problem even though the majority of school districts appear to be in compliance with CIPA requirements.

In general, districts are complying with CIPA. About 94% (128 of 136) of school districts surveyed were able to provide sufficient evidence to support the adoption of an Internet Safety Policy (ISP) and an Acceptable Use Policy (AUP) per CIPA requirements. There was sufficient evidence to show that Technology Protection Measures (TPMs) were in place at 80% (109 of 136) of school districts and were being utilized on all internet-capable devices provided to students and faculty. Nearly all school districts surveyed reported that they had not been cited for non-compliance and/or found in violation of CIPA regulations. Finally, 91% (124 of 136) of school districts reported that they set all school issued devices to "Safe Search" mode as recommended. These results are similar to those reported in the original review, which showed that each of the nine (9) districts tested had policies and TPMs in place.

Further analysis, however, shows that having policies and TPMs in place are not enough to protect students when not properly administered. When surveyed, only 19% (26 of 136) of districts were able to provide sufficient evidence showing that their ISP and AUP policies were enforced when devices were not located on school property. Fewer than half of school districts, 43% (58 of 136), had TPMs in place which alerted them to inappropriate online activities. Only 36% (49 of 136) of districts were able to provide sufficient evidence to show that they have given public notice or held a public hearing to discuss the policies and impacts of CIPA or the districts' ISP, AUP, and TPMs.

When it comes to monitoring devices or randomly testing them, the evidence is mixed. Only 17% (23 of 136) could provide sufficient evidence showing that they randomly test school issued devices to detect activity that is unusual or in violation of the ISP and/or AUP. Of those surveyed, only 59% (80 of 136) of school districts were able to provide sufficient evidence showing that they test and monitor TPMs.[4] Despite the efforts of many school districts, analysts determined the risks associated with the original findings have not been fully mitigated. As a result, the Government Accountability Division may revisit these risk areas in future reviews to ensure appropriate corrective action is taken.

[3] The population surveyed excluded all charter schools, schools under conservatorship during the review period (FY2020-2021), and specialty schools.

[4] The 80 school districts that are testing and monitoring, use a variety of TPM software vendors. Some school districts utilize as many as three (3) TPM software(s). Generally the type of reports being generated are the following: web filtering; email filtering; anti-virus; computer activity monitoring; cloud network security; malware; phishing; and monitoring for cyberbullying, depression, online predators. These systems allow school districts to monitor students for potential dangerous activity and are vital to student safety.

Spotlight: *Petal School District*

The Petal School District has reported success in the area of cybersecurity, so analysts interviewed district officials to learn more about what they are doing in their district to protect students in the hope that this information will be useful to other school districts.

Upon interviewing district officials, analysts learned that in conjunction with a content-filtering system, they also use a supplementary monitoring system which they believe has been invaluable. The monitoring technology tracks keystrokes by students on school computers, including when those computers are taken home. If the student types words that suggest they may engage in illegal activity or self-harm, the district is alerted. District leaders stated they needed an option that provided in-depth reporting to fully understand what the students are doing on school devices. It should be noted, that the state offers school districts a free content filtering software option, but according to district officials it is not adequate to meet the needs of the district. The Petal School District has been utilizing the supplementary monitoring software for 3-4 years. The district spends approximately $18,750 per year for the software, which is priced per device with an additional charge for monitoring by a dedicated agent from the monitoring company.

The monitoring company and human monitors work hand-in-hand with content filters to facilitate individual interventions. Alerts about incidents of threats, self-harm, violence, weapons, and pornography help schools provide informed interventions before it is too late. When the supplementary software detects at-risk words and phrases, it captures the screen and notifies designated staff via alerts or customized reports of at-risk language detected that day. The company's database, vetted by subject-matter experts, is pre-loaded with keywords and phrases in categories that indicate threats, violence, self-harm, and other at-risk behaviors. The database is customizable, allowing staff to monitor and respond in real time to issues as they appear.

In the past three years, Petal officials cited about 45 cases where counselors were able to make positive interventions. The most serious types of issues that the supplementary monitoring software picks up are: drugs, alcohol, sex, nudity, suicidal thoughts, weapons, and terrorism. The Petal Technology Coordinator stated that, "One thing that makes us different from other school districts is the cooperation between the technology department and the administration. I think what we do well here, is work exceptionally well together." The Petal Superintendent added, "Our proactive approach allows us to keep our kids, faculty, and staff safe. This system makes sense for our district and is something that is continuously vetted and monitored."