



Stacey E. Pickering
State Auditor

Performance Audit Division Brief:

Cybersecurity Audit
Review Vol. 9, No. 3
March 30, 2017

Introduction

A review of school districts conducted by the Office of the State Auditor (OSA) found an alarming number of students accessing pornography and other explicit material. OSA conducted the review of school districts' compliance with the Children's Internet Protection Act (CIPA) also known as the "Cybersecurity Audit" for the 2016-2017 school year. 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.

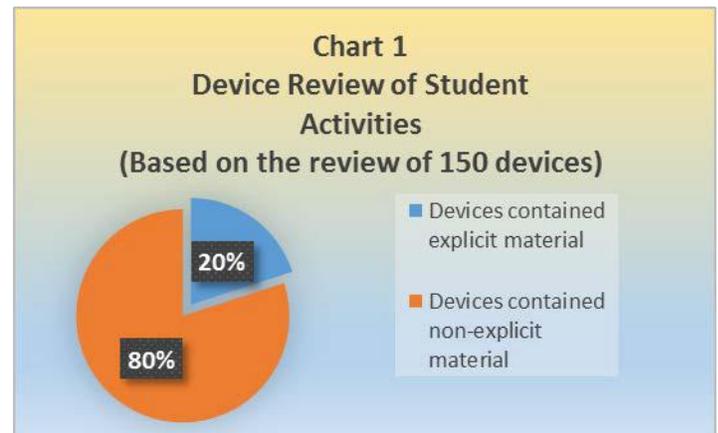
The purpose of the Cybersecurity Audit was to test the reliability of the security controls districts have in place and the filters, if any, installed on publicly owned devices that are issued and utilized by students across the State of Mississippi. OSA's objective was to ensure districts were protecting students from harmful and/or inappropriate material while accessing the Internet with these devices.

Under the CIPA requirements, school districts must have an Internet Safety Policy, Technology Protection Measures (TPM) in place, and provide public notices and hearings or meetings to address the proposed TPM and the Internet Safety Policy. TPM is a specific technology that blocks and filters Internet access to material that is considered obscene and/or harmful to minors. 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...*

School districts are accountable for the content that students are able to view and engage with while browsing the "World Wide Web" on school issued devices.

Audit Results

OSA created testing procedures to ensure effective policies of the school districts were formulated properly and that these policies were in compliance with CIPA and the Family Educational Rights and Privacy Act (FERPA). Of schools that participate in the One-to-One Initiative, OSA tested eighteen (18) schools within nine (9) school districts to ensure security controls of online activities were effective. During this process, 150 random devices were analyzed. ***Of the 150 devices tested, as indicated in Chart 1, 30 (20%) of the devices showed evidence that students were able to access explicit material on school issued devices; evidence also indicated that the district's filtering systems were ineffective when filtering inappropriate material.***



The nine (9) districts reviewed did not enforce their Internet Safety and/or Acceptable Use Policies by ensuring the TPM were effective while students had access to the Internet. In addition, OSA notes that of the nine districts reviewed, one (1) school district does not maintain TPM filtering when students are off school grounds.

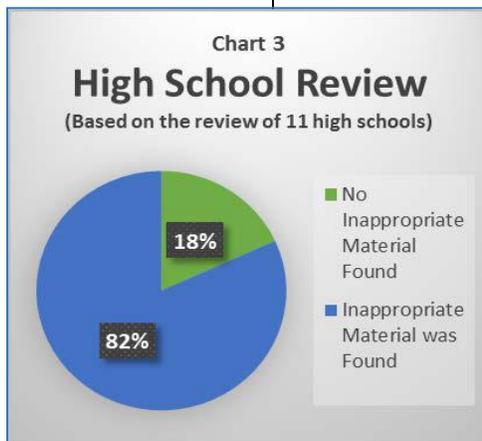
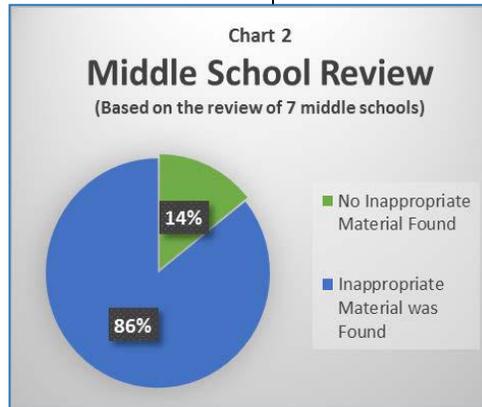


OSA also measured the districts' compliance of having an Internet Safety Policy which included TPMs that monitored the online activities of minors. It was determined that all nine (9) reviewed districts had a variety of written Internet Safety Policies and TPMs that block and filter devices issued to students; however, the audit discovered that there was inappropriate material found on student's devices and that districts do not appear to be completely adhering to their own policies.

Of the eighteen schools tested, seven were middle schools and eleven were high schools, as indicated in chart 2 and chart 3. Of these schools tested, six (86%) middle schools students' devices and nine (82%) high school students' devices contained explicit material such as pornography, even though the nine districts stated or presented documentation showing they have Internet Safety Policies in place. It appears the TPMs are not effective in warning district personnel of inappropriate online activities of students and therefore not effective in protecting students from accessing inappropriate material while on the Internet.

In light of the aforementioned findings, OSA makes the following recommendations:

- ***The Mississippi Department of Education (MDE) should provide districts with alternative solutions to evaluate the effectiveness of their monitoring system;***
- ***MDE should establish required uniform policies for all districts to follow regarding the installation of filtering packages and/or monitoring procedures;***
- ***MDE should establish a mandatory policy requiring schools districts to monitor devices off school grounds;***
- ***MDE should also establish substantial penalties for noncompliance;***
- ***As students are issued publicly owned devices, schools districts should utilize best practices to***



ensure they are constituting "good faith" to comply with CIPA;

- ***School Districts should test and monitor their TPMs periodically to ensure the safety of all students;***
- ***School Districts should have established detailed procedures showing how to implement safety protocols located within the district; and***
- ***School Districts should provide community outreach to inform parents on ways to keep students safe while online.***

In conclusion, OSA will continue to monitor school district's compliance with and report any discrepancies or school violations. School districts have a duty to be proactive in ensuring the safety of students that have access to the Internet through school issued devices. Districts should monitor individual devices to detect unusual activity, implement security best practices to maintain compliance with regulations, and provide detailed reports to parents to help in the monitoring process. The same security protocols and procedures should be in place while on campus or offsite. It is critical to keep students in safe places on the Internet and to closely supervise any open access to the Internet at all times.



The Office of the State Auditor
Post Office Box 956
Jackson, MS 39205-0956
Phone: 601-576-2800 in the Jackson area or
1-800-321-1275 Statewide
Fax: 601-576-2687*Website: <http://www.osa.state.ms.us>

The Performance Audit Division of the Office of the State Auditor assesses the performance of organizations, programs, activities, and functions of government in order to provide information to improve accountability, effectiveness, and to facilitate decision-making. All reports, documents, and supporting materials obtained and utilized by the Performance Audit Division will be considered public information, unless otherwise prohibited by law.

The Office of the State Auditor does not discriminate on the basis of race, religion, national origin, sex, age, or disability.