Cybersecurity is more important than ever in today's society, even more so in a public school environment. Ensuring that our students and staff data is secure is one of our biggest challenges. K-12 cybersecurity incidents have increased greatly over the last several years. There have been over 1100 incidents since 2016. There were 408 publicly-disclosed incidents in 2020 alone and that will only continue to increase. To ensure that we are using best practices we have joined the Multi-State Information Sharing & Analysis Center (MS-ISAC) and Cybersecurity and Infrastructure Security Agency (CISA). Both of these organizations offer free memberships to K-12 Schools and offer many tools and resources to enhance our cybersecurity.

In August of 2021 we began to utilize CISA Hygiene Services. CISA Hygiene Services provide two options to identify vulnerabilities and risks: 1) they scan all of our public IP addresses (port scanning) weekly, 2) they scan all of your public facing web servers (Web Application Scanning) once a month. Public IP addresses are those addresses that allow public access to our network. Public facing servers are those servers that we host and maintain for public access. SISK12, SISFIN and Cafeteria are a few examples of our public facing servers. When performing these scans, CISA sees where they can go and what they can access on our public facing network and servers and provides us with a report of what they find and how we can mitigate any identified risks.

We are pleased to report that so far all of the findings in both scans were at the level of medium risk or below; we had no critical or urgent issues to resolve. We have resolved several of the known issues and continue to review the reports and apply solutions at our weekly cybersecurity team meetings.