Finding 3: Information Technology Disaster Recovery Plan	
AG Finding Summary	The District had not established a comprehensive disaster recovery plan.
AG Recommendation	The District should establish a comprehensive IT disaster recovery plan that's includes the necessary critical elements and details and ensure that the plan is tested at least annually.
Original District Response	The District established a comprehensive IT disaster recovery plan effective December 2019 as recommended.
Status per Management as of July 2020	We have modified the IT Disaster Recovery Plan (IT DRP) to reflect enhancements to our backup and recovery procedures. These include changing to a powerful new backup software application in late 2019 that provides for faster recovery of servers and files. Changes also include the selection of a cloud service provider in February 2020 that provides cloud-based storage for backups as well as assistance in system testing and recovery. Using the cloud service provider's data center resources, backups can be rapidly restored and brought online for testing and recovery. Testing of server backups and restoration has been completed for critical servers, but the process should be adequate for all servers. At this time, backups of all high priority servers identified in the IT Disaster Recovery Plan (IT DRP) are copied to the cloud provider's data center immediately following the scheduled backup. Additional funding has been established in the FY 2021 preliminary budget and the plan will be to implement Disaster Recovery as a Service (DRaaS), including replication of critical servers, soon after October 1, 2020.