CCSESA
Technology Steering Committee
Cybersecurity Update

April 11, 2022

Eric Calderon
Technology Steering Committee (TSC) Chair
Chief Technology Officer
Riverside County Office of Education

Terry Loftus
Assistant Superintendent & Chief Information Officer
San Diego County Office of Education

David Thurston
Chief Technology Officer
San Bernardino County Superintendent of Schools

CCSESA

TSC: Leading Cybersecurity Efforts in CA

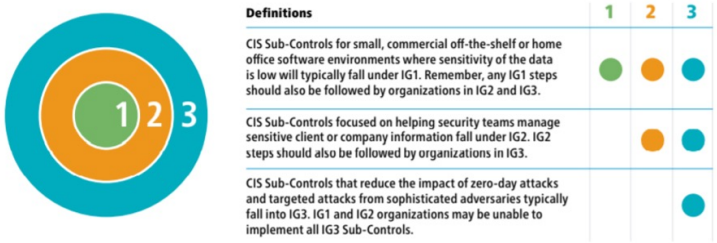
The TSC Cybersecurity Subcommittee brings together K-12 County Office of Education technology leaders and practitioners with the unified goal of ensuring that we are researching and implementing the strategies, technologies, processes, and policies needed **to effectively defend the data and infrastructure of statewide K-12 LEAs** (including state County Offices of Education, and their associated districts and charter schools).

We

- Research, implement, and share cybersecurity resources among TSC members.
- Create relevant materials that account for the diversity of our counties, districts, and regions.
- Develop and deliver professional development and awareness content for LEAs across the state.
- Advocacy at the local, state and federal levels. Whether it be for funding, adopted policies or direct partnerships (such as the current work with the California Military) the Cybersecurity Subcommittee seeks out resources and services that will benefit CoEs and our districts/charters.

Cybersecurity Solutions: CIS Framework

Align all members with a common cybersecurity framework: the Center for Internet Security (CIS) Controls and Safeguards. While member organizations may be a different places in their cybersecurity maturity journey, this no-cost framework allows for knowledge sharing and a common language that enhances collaboration. This framework can be leveraged by LEAs of all sizes, and with varying resources, including County Offices, Districts and Charter Schools.



The Center for Internet Security is responsible for the CIS Controls and CIS Benchmarks, which are globally recognized best practices for securing IT systems and data.

CIS is also home to Multi-State Information Sharing and Analysis Center (MS-ISAC) and is supported by the US Department of Homeland Security.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

CISA
CYBER+INFRASTRUCTURE

Cybersecurity Solutions: Training & Guidance

MFA

Multi-Factor Authentication

Multi-Factor Authentication is system that requires more than one distinct authentication factor for successful authentication. The three authentication factors are something you know, something you have, and something you are. **MFA is a proven approach in drastically reducing automated cybersecurity attacks**, with research from both Microsoft and Google noting that MFA blocks 99% of all automated account takeover (ATO) attacks.

On April 15th the TSC Cybersecurity Subcommittee is hosting the **2022 MFA Workshop**, which will be an informational and interactive session providing the needed strategies, processes, communication resources, and tools to implement MFA within their own organizations (CoEs).

This expertise will also empower CoEs in the future, as they provide support to their own districts/charters interested in adopting MFA.

Questions / Discussion