# Initial K-12 School Cybersecurity Controls for Small and Medium Schools with Mapping to Relevant Guidelines (DRAFT)

CERT Division

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

# Document Markings



This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.



DM23-0057

# Premise of multi-stage practices in native groupings

"The CPGs can help organizations that may lack the cybersecurity experience, resources, or structure in place to quickly identify and implement basic cybersecurity practices." This would seem to define most school districts, especially small and mid-sized organizations.

The K12SIX cybersecurity practice recommendations are organized by native groupings.
1.0 Sanitize Traffic to/from the Internet
2.0 Safeguard Student, Teacher, and Staff Devices
3.0 Safeguard Student, Teacher, and Staff Identities
4.0 Practice Continuous Improvement.

This is a workable structure on which:

- We can convey recommended cybersecurity practices in clear, cogent, and actionable.
- We can prioritize practices based on the recognition of resources constraints.
- We can move the districts over time to a more secure state.

# Example:
# 3.0 Protect Student, Teacher, Staff Identities

## Protect User Logins

- Configure passwords for length, strength, expire, and reuse [CPG 1.4, K12SIX 3.2]
- Detect unsuccessful login attempts [CPG 1.1A]
- Enforce account lockout for unsuccessful login attempts [K12SIX 1.1B]
- Revoke credentials for departed employees [CPG 1.7]
- Separate user and privileged accounts [CPG 1.5]

❖Implement Multi-Factor Authentication [CPG 1.3, K12SIX 3.1]

Multi-Factor Authentication is an example where other, related, and workable actions can precede a significant project and potentially costly implementation and operation. MFA is a solution that can provide measurable mitigation of cyber risk. However, MFA will not deploy or manage itself, has internal as well as external costs, and predominantly addresses authentication for remote network access, not for internal access or application-direct access. Although MFA is a formidable solution, it doesn't alone solve for all student, teacher, and staff identity risks.

# Each practice moves a district toward true north

Multi-stage practices help to move an organization to a better cyber state.

For the Grouping, Protect Student, Teacher, and Staff Identities, each iterated practice is accretive to Protect User Logins and:

- Would not be replaced by MFA
- Could coexist with MFA, for internal network or application authentication
- Are low-cost, low-complexity solutions
- Are aligned with CPGs
- Are organized by K12SIX Native Groupings
- Provide positive feedback for district cybersecurity practitioners

# Sources for multi-state practices

In this deck, nearly all multi-state practices are aligned with existing cybersecurity practice recommendations from

- CISA CPGs
- CISA K-12 Cyber Act Report
- K-12 SIX Recommendations, Reports

# Exceptions to source alignment

Exceptions fall in two categories

- Practices for Operational Technology

  Some CPGs are inherently focused on the relationship of IT to OT and the particular cyber risks faced by OT.

  These relationships and risk have been excluded from reference.

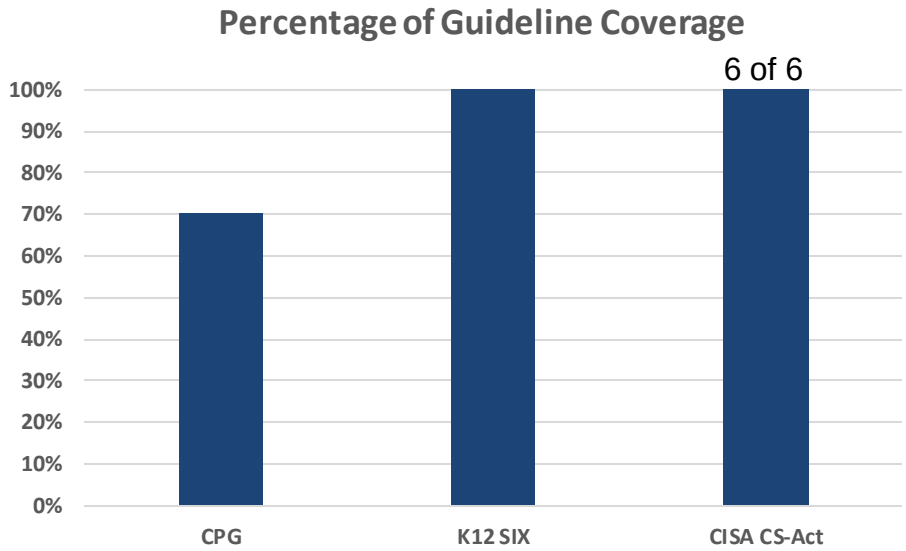
- Practices for data security/protection

  CPGs recommend only two practices specific data security/protection.

  Two other practices refer to the protection and preservation of particular data that may be included in activity logs. These two practices have been excluded.

# Practices per source



| CPGs excluded | Reason |
| --- | --- |
| 2.2 Disable macros by default<br>3.1 Log collection<br>3.2 Secure log storage<br>5.2 Vulnerability disclosure/reporting<br>5.3 Deploy security.txt files<br>7.4 Document network topology<br>8.2 Detecting relevant threats and TTPs | Beyond capability of most small to medium K-12 schools |
| 4.2 OT cybersecurity leadership<br>4.4 OT cybersecurity training<br>4.5 Improving IT and OT cybersecurity relationships<br>5.5 Limit OT connections to public Internet | OT-specific capability irrelevant for K-12 schools |

Following are the remaining K12SIX Native Groupings.

Each has been assigned multi-stage practices.

# 1.0 Sanitize Network Traffic to/from the Internet

Employ email security [CPG 8.3, K12SIX 1.2]

Block malicious and other web content by category and source [K12SIX 1.1]

Segment internal network access by asset criticality [CPG 8.1, K12SIX 1.3]

Forbid exploitable vulnerabilities on the Internet [CPG 5.4]

# 2.0 Safeguard Student, Teacher, Staff Devices

Change default passwords [CPG 1.2]

Use unique credentials and avoid shared accounts [CPG 1.6]

Restrict user and administrative access to least privilege [K12SIX 2.1]

Employ hardware and software approval process [CPG 2.1]

Collect (critical) asset inventory [CPG 2.3]

Document approved device configurations [CPG 2.5]

Prohibit connection of unauthorized devices [CPG 2.4]

Apply updates and patches to mitigate known vulnerabilities [CPG 5.1, K12SIX 2.2, K12SIX 4.1]

# 4.0 Practice Continuous Improvement

Organize for cybersecurity leadership [CPG 4.1]

Employ cybersecurity training [CPG 4.3, K12SIX 4.3]

Procure appropriate and secure IT solutions [CPG 6.1, K12SIX 3.3]

Seek third-party validation of cybersecurity effectiveness [CPG 5.6]

Require supply chain incident reporting [CPG 6.2]

Require supply chain vulnerability disclosure [CPG 6.3]

Report confirmed cybersecurity incidents to external entities [CPG 7.1]

Develop and test incident response plan [CPG 7.2, K12SIX 4.4]

Prepare and test system backups [CPG 7.3]

# New Grouping: Manage Sensitive Data
# Intended to address K12SIX 4.2

Classify sensitive data [None]

Locate sensitive data in structured and unstructured stores [None]

Enact policies to regularly backup, archive, and/or delete sensitive data and documents [K12SIX 4.2]

Apply encryption at rest and in transit for sensitive data [CPG 3.3]

Segment internal network to cordon off sensitive data stores [CPG 8.1]

Control exposure of sensitive data to the internet [CPG 3.4]

This new grouping would come after current K12SIX 3.0.
Current K12SIX 4.0, "Practice Continuous Improvement" would become 5.0