June 11, 2024

Cybersecurity: Administrative Controls

(Policies and Standards)

Krissy Cross (kristina.cross@arkansas.gov)
Jeff Killingsworth (jeff.killingsworth@ade.arkansas.gov)
Ray Girdler (raymond.girdler@arkansas.gov)

Agenda

01 Introductions: Presenters & Purpose

02 ADE: Act 504 & Cyber Response Board Updates

03 DIS: Sample Policy & Standard Review

04 DIS: NIST SP800-53/53B Overview & Resources

05 Strategic Planning

06 Next Steps

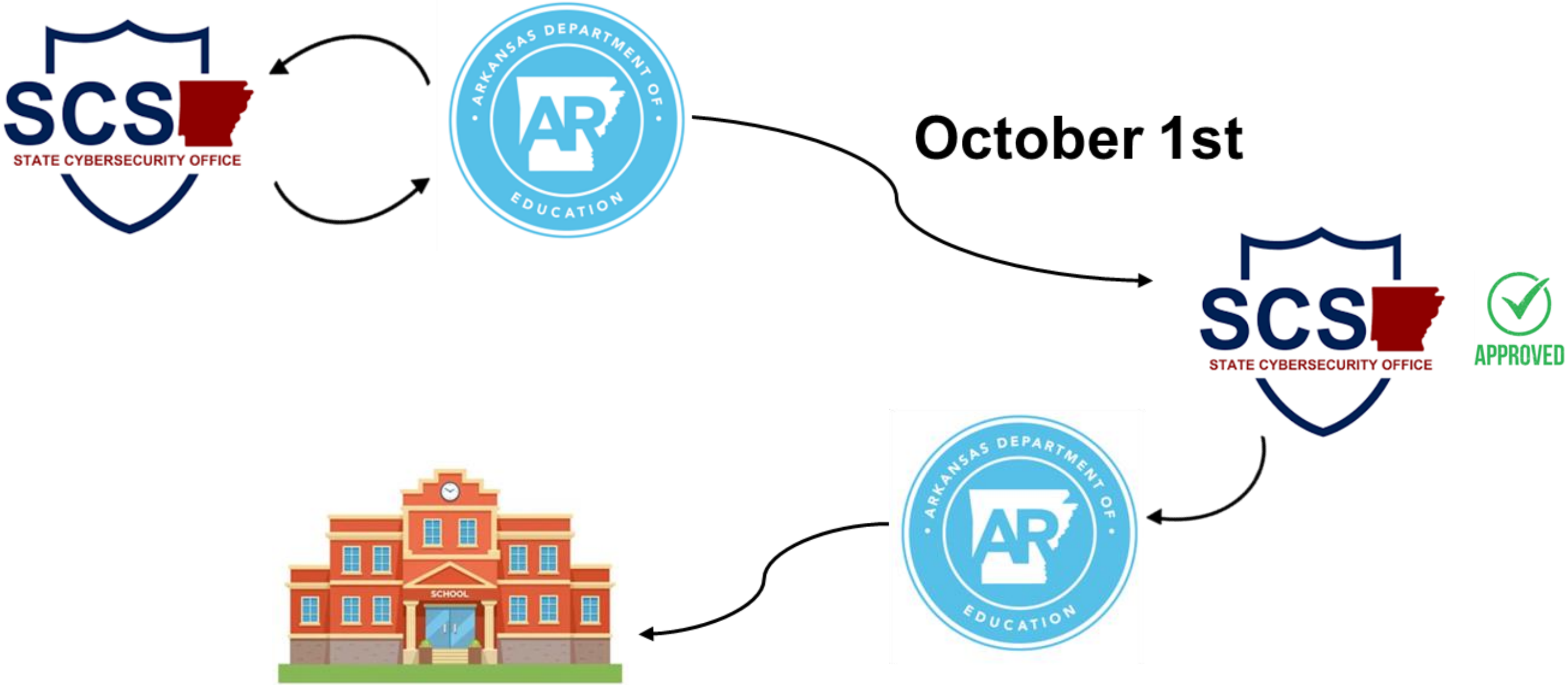
ADE

Act 504

Act 504

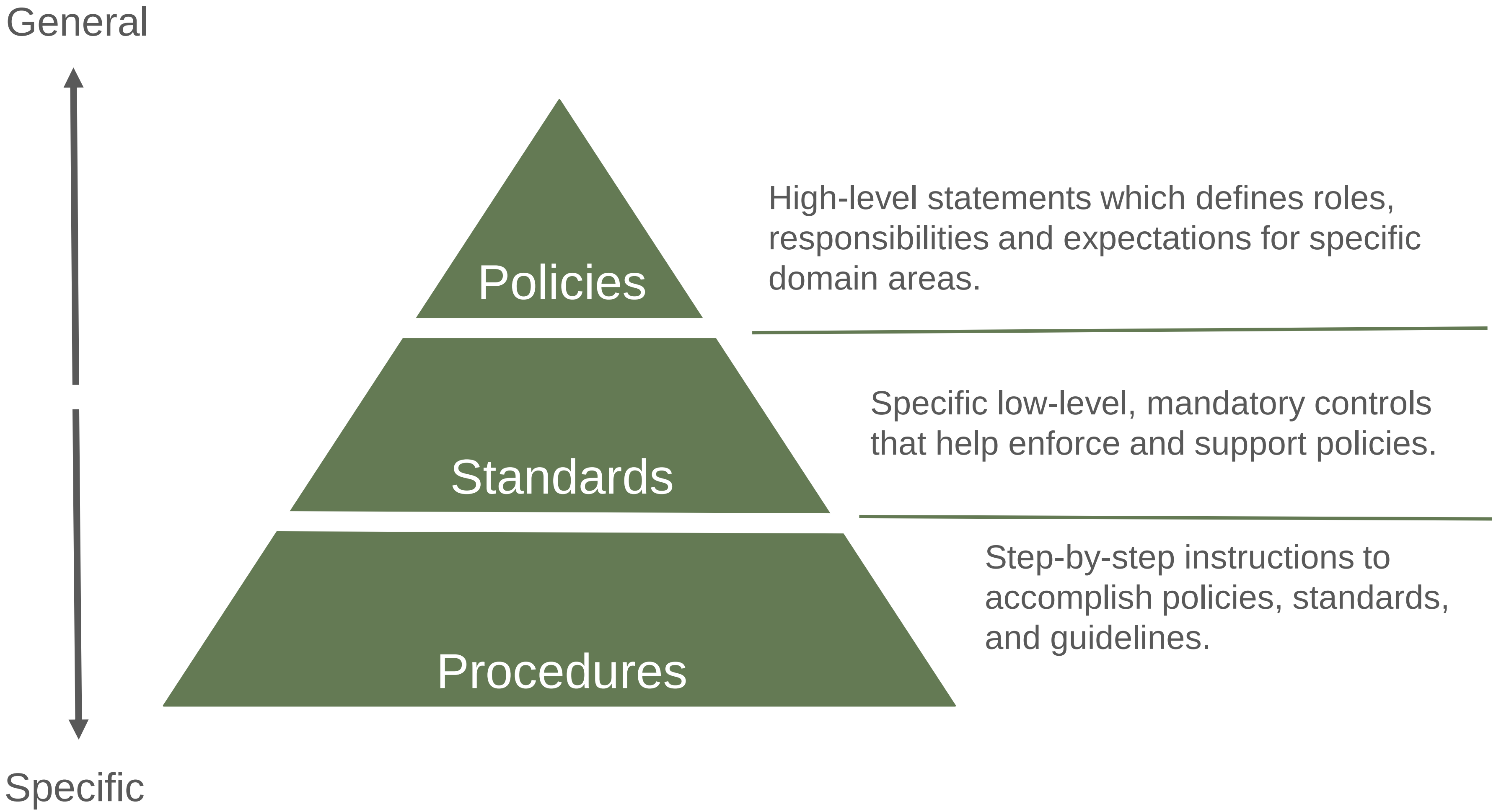
- Technology Resources Policy (Commissioner’s Memo)
- Cybersecurity Policy

Act 504 Timeline



October 1st

SCS
STATE CYBERSECURITY OFFICE
ARKANSAS DEPARTMENT OF EDUCATION
AR
SCS
STATE CYBERSECURITY OFFICE
APPROVED
ARKANSAS DEPARTMENT OF EDUCATION
AR
SCHOOL



General

Policies

High-level statements which defines roles, responsibilities and expectations for specific domain areas.

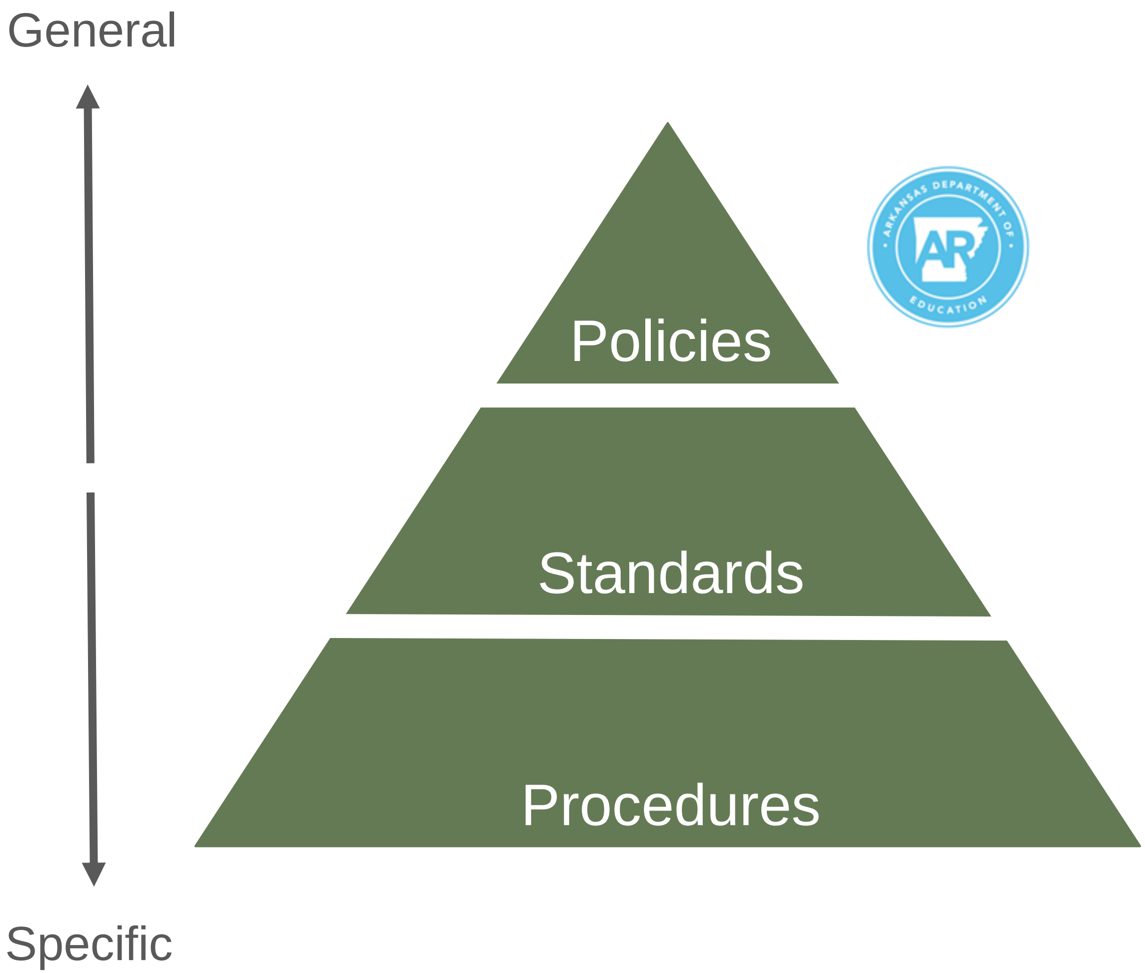
Standards

Specific low-level, mandatory controls that help enforce and support policies.

Procedures

Step-by-step instructions to accomplish policies, standards, and guidelines.

Specific



General

Policies

Standards

Procedures

Specific

ADE

Act 846

Act 846

Arkansas Self-Funded Cyber Response Program

- Administered by the Arkansas Cyber Response Board
- All counties, municipalities, and public school districts must participate
- Maximum of $300,000 contributed by each group for each of the first 2 years

Act 846 cont.

Program Coverage

- Not to exceed $100,000 in actual losses
- Does not cover a ransom payment
- Amount of coverage can potentially be lower based on the board's minimum cybersecurity standards

Act 846 cont.

Minimum Standard Categories

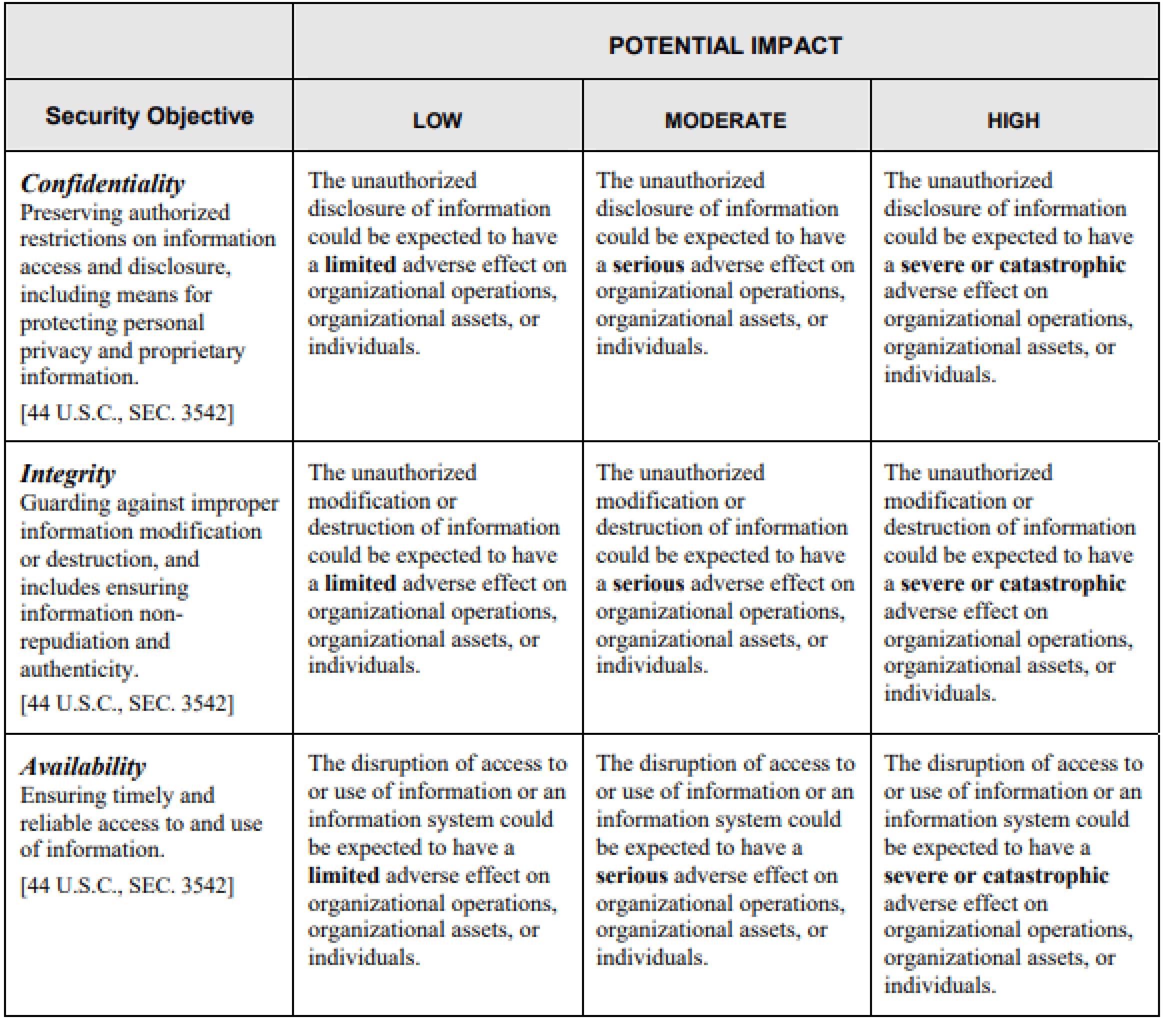
- Multi-Factor Authentication (MFA)
- Offline Data Backups
- Cybersecurity Awareness Training
- Password Standards
- Patch Management

DIS

Policies & Standards

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

NIST SP800-60



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Fun Facts

- NIST CSF ≠ NIST SP800-53
- 287 Moderate NIST SP800-53 Controls
- The first control in each control family is establishing a written policy.
- A security breach is almost always the result of either a missing or ineffective control.
- NIST SP800 series alone currently has 212 publications.

Samples

- Sample Policy
- Policy Summary (DRAFT)
- Sample Standard

Resources

- NIST SP800-53
- NIST SP800-53B
- Cybersecurity and Privacy Reference Tool
- NIST SP800-53 (3rd party site)
- NIST SP800-53 and SP800-53B Spreadsheets

Meeting Goals for Today

01 Understand processes, roles, commitments, and flexibilities

02 Prioritize NIST control families (high to low)

03 Establish a timeline for standards development

02 Establish a process/flow, strategy (draft>review>approve), and responsible persons

Next Steps

- (insert new meeting date) - (insert person responsible)

June 11, 2024

Cybersecurity: Administrative Controls

(Policies and Standards)

Krissy Cross (kristina.cross@arkansas.gov)
Jeff Killingsworth (jeff.killingsworth@ade.arkansas.gov)
Ray Girdler (raymond.girdler@arkansas.gov)