Appendix A

Links to Extra Resources

Below you will find links or references to resources, which will help expand on topics covered in this webinar. These links are provided for reference only and do not represent endorsement by the State of Arizona Office of the Auditor General or guarantee that the controls discussed are the only or appropriate methods for your environment. Note that references to NIST 800-53 would also be covered by Arizona Department of Administration Arizona Strategic Enterprise Technology's (ADOA-ASET) Policies and Procedures, available here: https://aset.az.gov/resources/policies-standards-and-procedures

Slide 7 — US Department of Education privacy resources

- U.S. Department of Education Privacy Technical Assistance Center (PTAC)
- Data Breach Response Checklist

Slide 9 – Firewalls

- SANS Critical Security Control 11
- NIST 800-53: SC-7
- NIST 800-41
- NSA Top 10: Limiting Workstation-to-Workstation Communication

Slide 10 – Security Software and Appliances

- SANS Critical Security Control 5
- NIST 800-53: SI-3, SI-4

Slide 11 – Administrative Privilege Restrictions

- SANS Critical Security Control 12
- NSA Top 10: Control Administrative Privileges

Slide 12 – Software Controls

- SANS Critical Security Control 2
- NSA Top 10: Application Whitelisting
- NIST 800-53: CM-7

Slide 13 – VPN

- NIST 800-53: AC-17
- NIST 800-46

Slide 14 – Remote System Control

- NIST 800-53: CM-7

Slide 15 – Encryption

- NIST 800-53: SC-28
- NIST 800-111

Slide 16 – File Share Controls

- NIST 800-53: AC-1, AC-2, AC-3, AC-6

Slide 17 – Login Banners

- NIST 800-53: AC-8

Slide 19 – Vulnerability Management

- SANS Critical Security Control 4
- NIST 800-53: RA-5

Slide 20 – Patch Management

- NIST 800-53: SI-2, SI-5
- NIST 800-40
- NSA Top 10: Take Advantage of Software Improvements

Slide 21 – Configuration Management

- NIST 800-53: Configuration Management Family (CM)
- NIST 800-128

Slide 22 – Logging and Monitoring

- SANS Critical Security Control 14
- NIST 800-53: AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9

Slide 23 – Web Content Monitoring

- Arizona Revised Statues: §34-502
- Arizona Revised Statues: §38-448

Slide 24 – Wireless Access Points

- SANS Critical Security Control 7
- NIST 800-53: AC-18, SC-8, SC-13
- NIST 800-153

Slide 25 – End-of-Life Systems

- NIST 800-53: SA-22

Slide 26 – Hardware Disposal

- U.S. Department of Education – Best Practice for Data Destruction
- NIST 800-88

Slide 27 – Email Security

- NIST 800-45

Slide 28 – Vendor / Cloud Services

- U.S. Department of Education – Cloud Computing
- NIST 800-144
- NIST 800-145
- NIST 800-146

Slide 29 – Incident Response

- U.S. Department of Education – Data Breach Response Checklist
- SANS Critical Security Control 18

Slide 30 – Bring Your Own Device (BYOD)

- SANS Critical Security Control 1 and 3
- NIST 800-124