Tab 26

Overview of Recent Audit Reports

Coordinating Board for Higher Education
March 6, 2019

BACKGROUND

MDHE undergoes routine annual audits by the following entities:

1) State Auditor's Office (SAO) - The SAO determines which state funds have the most significant amount of activity and tests transactions from those funds during its audit of the statewide financial statements. Both the loan program and the state financial aid funds typically have activity at a level that the SAO considers significant and those funds are included in test work for the comprehensive annual financial report (CAFR).

2) United States Department of Education (USDE) – The USDE performs on-site reviews of the Missouri Student Loan Program (MSLP) information security controls on a periodic basis, as well as requires the department to submit self-assessments of information security controls each year.

3) RubinBrown – Through a contract awarded by the Office of Administration, RubinBrown audits the MSLP's annual comparative financial statements. An independent audit is required by the USDE of all guaranty agencies; the department must submit a copy of its audited financial statements to the USDE each year.

CURRENT STATUS

The SAO released its CAFR in January 2019. The department had no findings. The full report is available here for review.

The USDE issued its Security Control Review to the department in January 2019. In total, 77 security controls in 18 control families were reviewed and MDHE received the highest possible rating in all 18 control families. There was one finding, which related to the department's vulnerability scans, that all guaranty agencies had. Over 1600 vulnerabilities were discovered at the time the review was conducted in July 2018. The department strengthened monitoring of our vulnerabilities through receiving monthly reports and more closely tracking specific threats, as well as taking necessary steps when remediation of identified threats could be achieved. Through our work with OA-ITSD, the latest vulnerability scan in February 2019 identified only 56 vulnerabilities. The full report is attached for review.

RubinBrown issued its final report to the department in December 2018. As outlined during the call-in to the Audit Committee work session in December 2018, the department had no findings. The full report is attached for review.

NEXT STEPS

With regard to the finding on the USDE Security Control Review, the department will continue to work closely with OA-ITSD to identify, track, monitor, and remediate vulnerabilities that show up on the monthly scan.

RECOMMENDATION

This is an information item only.

ATTACHMENTS

A. USDE Security Control Review
B. RubinBrown Audit Report

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of the AMERICAN MIND®

MDHE SA Findings Report
Security Control Review

2018-09-07

Version 1.0 FINAL

Document Version Control

VERSION	DATE	AUTHOR	DESCRIPTION
0.1	2018-08-31	BC Team	Initial document preparation.
0.2	2018-09-04	BC Team	Released for MDHE Review.
0.3	2018-09-06	MDHE	Completed Appendix A.
1.0	2018-09-07	BC Team	Finalized for signatures.

Table of Contents

Section 1 Guaranty Agency Points of Contact

The MDHE information system points of contact for the 2018 Onsite Review include the following.

1.1. Executive Director

Marla Robertson
marla.robertson@dhe.mo.gov

1.2. Information Technology Contact

Robert Powell
robert.powell@dhe.mo.gov
(573) 526-0173

1.3. Secondary Contact

Jeff Ferguson
jeff.ferguson@oa.mo.gov

Section 2 Introduction

In support of the Federal Student Aid (FSA) Security and Privacy (S&P) Program, the Blue Canopy Group, LLC (Blue Canopy) Security Assessment (SA) Team conducted an independent Security Control Review on the information system.

2.1. Scanning Activities

During the security control review, the SA team observed vulnerability and compliance scanning activities conducted by MDHE personnel Tuesday, July 10, 2018 - Thursday, July 12, 2018 against the information system at the operating system, database, web, and network device layers. This report documents the findings of the vulnerability scanning and other security assessment activities. A member of the Vulnerability Scan Analysis Team accompanied the assessors to validate the vulnerability scan solution is configured to meet the requirement of the NIST 800-53 Rev.4 RA-5: Vulnerability Scanning control requirements. This provides the stakeholders with actionable recommendations in order to remediate vulnerabilities and reduce risk.

2.2. Security Control Review

The SA team also performed control testing using NIST 800-53A Revision 4 test cases, using the FSA critical NIST control baseline, to evaluate the information system for compliance with NIST. The findings associated with the controls evaluated are listed below. As an attachment, the SA team provided the Security Requirements Traceability Matrix (SRTM) which provides more detail into how the control compliance was determined. This report also provides recommendations for how to remediate these findings.

Section 3 Executive Summary

The remediation recommendations are included in this report, aggregated by finding ID. This produces a single remediation recommendation entry for each finding (one finding ID with multiple affected hosts). After this process, the SA team performed additional analysis on the findings to identify:

- Any previously reported findings
- Findings released during the current patching cycle
- Hosts with a disproportionate share of vulnerabilities (outliers and anomalies)

This review ensures that the report accurately reflects the actual risk to FSA data.

3.1. Scan Statistics

Personnel conducted the vulnerability and compliance scans during the security review, Tuesday, July 10, 2018 - Thursday, July 12, 2018, and results provided to the SA team.

- **Scans Completed:** (OS / DB / Web / Network)
- **Targets Scanned:** 91
- **Individual Findings Discovered[1]:** 1604

The personnel validated the scanner configuration before scanning and compared the scanned targets to the boundary documentation to ensure comprehensive scanning of the information system.

3.2. Scan Finding Analysis

The SA team did not receive a follow-up scan during the remediation window; therefore the following information is not applicable:

- **Individual Findings Closed in the Follow-Up Scan:** N/A
- **False Positives Verified and Closed:** N/A

Section 4 Third Party/ External Vendor Security Summary

The SA teams analyzed Evidence Request List response evidence and conducted on-site interviews related to implementation of NIST security controls (AC-20, PS-7 and SA-9). The analysis has resulted in a determination that MDHE is satisfying these NIST security control requirements of overseeing third party and external entities as they to “Use of External Information Systems”, “Third-Party Personnel Security” and “External Information System Services.” Please see the MDHE Security Requirements Traceability Matrix (SRTM) for the complete testing results of these controls. Great Lakes Higher Education Corporation (GLHEC) is the only known third party servicer used by MDHE at this time.

[1] Before Aggregation by Finding ID.

Section 5 Finding Summary

5.1.1. Analysis Criteria

The Guaranty Agencies (GAs) were first provided a draft report with an initial rating/score that was solely established on an objective scoring methodology that was normalized and uniform so that any one question, control, or control family was assessed equitably. FSA then conducted phone interviews with each GA. Upon the conclusion of each GAs phone interview, FSA subject matter experts (SMEs) made a subjective determination of the GAs rating/score, taking into consideration the phone interview feedback. Rating criteria are based on two metrics:

1. Assessed Security Control Effectiveness
2. Feedback from Onsite Visits

EFFECTIVENESS OF THE GA RESPONSE IN MEETING THE SECURITY OBJECTIVE	STRENGTH OF EVIDENCE IDENTIFIED IN MEETING THE SECURITY COMPLIANCE REQUIREMENT
Good	➢ Security Control is Satisfied ➢ Assessment evidence satisfactory and interview notes validate the security control ➢ ***Score***: >= 80%
Medium	➢ Security Control is Satisfied or Partially-Satisfied ➢ Assessment evidence and interview notes provide reasonable assurance in validating security control is mostly implemented ➢ ***Score***: >= 60% to < 80%
Poor	➢ Security Control is Partially-Satisfied or Not Satisfied ➢ Assessment evidence and interview notes provide reasonable assurance in validating security control is somewhat implemented ➢ ➢ ***Score***: >= 30% to < 60%
Critical	➢ Security Control is Partially-Satisfied or Not Satisfied ➢ Assessment evidence is not provided and/or interview provide no reasonable assurance that security control is implemented ➢ ***Score***: 0% to < 30%

Based on the GA's responses to the “Evidence Request List” that was submitted, the objective scoring methodology, and results of the onsite visits, a rating was provided for each security control and then an overall rating of Good, Medium, Poor, or Critical was calculated for each security control family.

5.1.2. Control Family Scores

Control Family Name	2017 Self-Assessment Rating Per Security Control Family
Access Control (AC)	Good
Security Awareness and Training (AT)	Good
Auditing and Logging (AU)	Good
Security Assessments (CA)	Good
Configuration Management (CM)	Good
Contingency Planning (CP)	Good
Identification and Authentication (IA)	Good
Incident Response (IR)	Good
Maintenance (MA)	Good
Media Protection (MP)	Good
Physical and Environmental (PE)	Good
Security Planning (PL)	Good
Personnel Security (PS)	Good
Risk Assessment (RA)	Good
Systems Acquisition (SA)	Good
System and Communications Protection (SC)	Good
System and Information Integrity (SI)	Good
Privacy (AP, AR, DI, DM, IP, SE, TR, UL)	Good
Overall Rating	Good

Control Family Name	2018 Onsite Review Rating Per Security Control Family
Access Control (AC)	Good
Security Awareness and Training (AT)	Good
Auditing and Logging (AU)	Good
Security Assessments (CA)	Good
Configuration Management (CM)	Good
Contingency Planning (CP)	Good
Identification and Authentication (IA)	Good
Incident Response (IR)	Good
Maintenance (MA)	Good
Media Protection (MP)	Good
Physical and Environmental (PE)	Good
Security Planning (PL)	Good
Personnel Security (PS)	Good
Risk Assessment (RA)	Good
Systems Acquisition (SA)	Good
System and Communications Protection (SC)	Good
System and Information Integrity (SI)	Good
Privacy (AP, AR, DI, DM, IP, SE, TR, UL)	Good
Overall Rating	Good

5.1.3. Remediation Recommendations

To ensure that all control families achieve a compliance rating of “Good” this section provides high level recommendations. Risk Assessment control implementations should reflect the guidance provided in NIST publications.

Section 6 Findings

6.1. FINDINGS REQUIRING DISCUSSION

Multiple Vulnerabilities Found (RA-5)		
NIST SP 800-53 Control: RA-5	**Type:** Corrective Action	**Risk: VERY HIGH**
Affected Asset(s): 1604 Vulnerabilities Discovered		
Status: Additional Analysis Required		
Finding Description: SCA Finding: 'Multiple vulnerabilities found (RA-5)' Affected Asset(s): RA-5: Vulnerability Scanning Instance Detail: Nexpose results show the following vulnerabilities for MDHE: Critical – 1104 Severe – 448 Moderate – 54 Total - 1604		
Threat Description: Vulnerabilities could be exploited by unskilled attackers.		
Recommendation: Remediate all vulnerabilities within defined frequencies that are commensurate with the level of risk the vulnerabilities present.		
Stakeholder Discussion: [To be completed by Stakeholder]		

Section 7 Signature Page

CISO Recommendations:

- Concur with Assessment team's GA Review
- The GA needs to ensure that:
    - Monthly CAP updates are obtained from MDHE .
    - Ensure that all documentation is updated to reflect changes in the environment and that the environment is properly described.

_____ _____

Daniel Commons Date
Director, IT Risk Management
Chief Information Security Office (CISO)
Federal Student Aid (FSA)
U.S. Department of Education

Appendix A MDHE Security Onsite Review Analysis CAP

Due to FSA Wednesday, September 04, 2019

Purpose: This Corrective Action Plan (CAP) describes the Security Onsite Review findings based upon the responses of partially or not satisfied security control implementation and describes progress towards addressing the findings. Provide enough information in your planned corrective actions to enable the analyst to understand the planned remedy, including specific actions to close the finding, compensating controls either in place or planned, or reason for acceptance of the risk of not remediating the finding.

- ***Threat Level Assigned By The Analyst***: Based on the possible risk to the Agency if the failed security control is not remediated
  - Very High
  - High
  - Moderate
  - Low
- ***Agency Concurs With Recommended Remediation***: Concur or does not concur
  - ***If The Agency Does Not Concur***: The compensating/mitigating controls or risk acceptance approach must be stated in planned corrective action
- ***Status***: Status of the finding remediation/mitigation effort
  - ***NS*** = Not Started
  - ***U*** = Underway
  - ***C*** = Completed
- ***Expected Completion Date***: Expected date the finding will be remediated; include any planned milestones

A.1. Risk Assessment (RA)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
RA-5	Multiple vulnerabilities found.	Remediate all vulnerabilities within defined frequencies that are commensurate with the level of risk the vulnerabilities present.	VERY HIGH	Concur	OA-ITSD runs Nexpose reports monthly and works to address vulnerabilities by level of risk. Patches are applied to the environment weekly, and can be applied sooner depending on level of severity.	Vulnerability remediation is an ongoing process. A new report is ran and reviewed monthly. The number of vulnerabilities have gone down greatly from 7/2018 scan due to patches and new computer placement. Current vulnerabilities from a 9/6/18 Nexpose report are: Critical: 15 Severe: 25 Moderate: 22 Total: 62	9/4/19