Tab 27

Overview of Recent Audit Reports

Coordinating Board for Higher Education
December 9, 2020

BACKGROUND

DHEWD undergoes routine annual audits by the following entities:

1) State Auditor's Office (SAO) – The SAO determines which funds have the most significant amount of activity and tests transactions from those funds during its annual Statewide Financial Statements Audit (SEFA). Within DHEWD, the loan program, the state financial aid funds, and federal funds administered by the Office of Workforce Development typically have activity at a level that the SAO considers significant. The SAO conducts the SEFA of these funds and includes the findings in its 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, as well as requires the department to submit self-assessments of information security controls each year.

3) CliftonLarsonAllen, LLP – Through a contract awarded by the Office of Administration, CliftonLarsonAllen, LLP 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

State Auditor – 2020

The State Auditor is currently conducting an audit of the DHEWD loan program, sampling some GR funds against the DHEWD internal control plan, and reviewing other federal funds (not WIOA) for the CAFR. DHEWD staff continue to work with the State Auditor daily, providing requested information.

USDE Program Audit of DHEWD – 2019

USDE conducted its Program of Review of DHEWD from September 17, 2019, through September 19, 2019, for the period of October 1, 2017, through September 30, 2018. The draft report identified one finding. DHEWD provided a copy of the report during the June board meeting. The finding identifies an issue with the DHEWD contract with Ascendium. USDE believes that DHEWD's contract with Ascendium asks Ascendium to do both default aversion and post default collections, in violation of 34 CFR 682.404(j)(4). DHEWD submitted its response to the finding on June 1, 2020, and provided a copy of its response to the CBHE at the September board meeting. To date, DHEWD has not received a response to its submission.

USDE Information Security Audit- 2019

DHEWD staff continue to work with the USDE on resolving findings in the USDE Information Security Audit. There are three findings remaining, CP-4 was due by July 7, 2020, and RA-5 and SI-2 are due by September 7, 2020. CP-4 is related to the ITSD disaster recovery testing exercise that is required. Due to the ongoing COVID-19 situation, ITSD postponed the exercise. The Loan DR testing began October 27, 2020, and is currently ongoing but we expect it to conclude November 6, 2020. DHEWD sent a CAP Update to USDE July 7, 2020, to identify the DR exercise was postponed due to COVID-19. USDE has not indicated it has any issue with the delay. RA-5 and SI-2 are both related to vulnerability testing. DHEWD and ITSD implemented a new software called Nessus and are now conducting and resolving vulnerability tests. By the end of November,

DHEWD will supply evidence that it is conducting scans. DHEWD will not provide the actual vulnerability scans themselves. It remains to be seen whether USDE will close the findings without receiving the actual scans.

USDE Information Security Self-Assessment – 2020

Guaranty Agencies that did not have an on-site audit in 2020 completed a 2020 Self-Assessment of their security controls. DHEWD staff originally had between February and May of 2020 to complete the self-assessment. Due to the COVID-19 crisis, the completion deadline was extended until July 31, 2020. DHEWD completed and submitted the self-assessment on all 256 NIST Controls on time. The USDE contractor, Blue Canopy, provided a draft Self-Assessment Security Review Report dated August 25, 2020. A copy of the report was provided during the September board meeting. The report provides an overall rating of DHEWD as "good." There are 21 findings noted. DHEWD received the Final Security Review Report (attached) on November 20, 2020 noting that all findings as resolved. There are no outstanding audit issues with the self-assessment.

Clifton Larson Allen (CLA) Audit

CLA conducted its interim field work for the annual independent audit of the financial statements and is presenting its update to the CBHE today.

Office of Inspector General (OIG) – United States Department of Education

The OIG is conducting its first audit of the State of Missouri's administration of the Governor's Emergency Education Relief (GEER) Fund grant. The audit will review our awarding process and planned monitoring process. The audit will continue into January of 2021.

NEXT STEPS

State Auditor – 2020

DHEWD will continue to work with the State Auditor on all pending audits.

USDE Program Audit of DHEWD – 2019

DHEWD will continue to work with USDE to find an acceptable corrective action to the single finding in the USDE Program Review of DHEWD.

USDE Information Security Audit – 2019

DHEWD will continue to provide the USDE corrective action plans as scheduled required in the DHEWD response to the USDE Information Security Audit.

Office of Inspector General (OIG) – United States Department of Education

DHEWD staff will work with DESE staff to comply with the OIG audit.

RECOMMENDATION

This is an information item only.

ATTACHMENTS

A. CLA Audit Report
B. USDE Information Security Self-Assessment Final Security Review Report

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

PROUD SPONSOR of the AMERICAN MIND®

Missouri Department of Higher Education and Workforce Development (MDHEWD) Guaranty Agency (GA) FY20 GASATRAQ Self-Assessment

GA Security Review Report (SRR)

Friday, November 20, 2020

Version 1.0 (Final)

Delivered by JACOBS Technologies Inc.

Document Version Control

Version	Date	Author	Description
0.1	2020-11-18	Blue Canopy Team	Initial version.
0.2	2020-11-19	Blue Canopy Team	Quality Assurance review (Peer).
0.3	2020-11-19	Blue Canopy Team	Quality Assurance review (Team Lead).
0.4	2020-11-19	Blue Canopy Team	Management review.
1.0	2020-11-20	Blue Canopy Team	Released for FSA/ GA-MDHEWD for review and signature.

Contents

Tables

1 Introduction

1.1 Background

Starting in 2017, Federal Student Aid (FSA) required all Guaranty Agencies (GAs) to complete a Security Self-Assessment by the Agency to identify the GA's official Information System (IS) security posture baseline. The intent of the GA Self-Assessment is to ensure GAs meet NIST security standards with plans to support broader cybersecurity-related programs, initiatives, and functions.

Each year, FSA selects a group of GAs to complete this self-assessment.

1.2 Scope and Methodology

In support of the FSA Security and Privacy (S&P) Guaranty Agency Security Assessment (GASA) Program, the Missouri Department of Higher Education and Workforce Development (MDHEWD) conducted a self-assessment of the MDHEWD information system using FSA's GASATRAQ 2.0 ("GASATRAQ") tool.

Testing methodologies consisted of GA personnel conducting a self-assessment of the FSA-selected security controls (see Table 1: Controls Reviewed). The Blue Canopy Group, LLC ("Blue Canopy") Security Assessment (SA) Team ("SA Team") then conducted an independent Security Control Review of the responses received, including reviewing supporting artifacts uploaded into the GASATRAQ self-assessment tool. The SA Team uses NIST SP 800-53A to determine if a control is effectively implemented and operating as intended.

1.3 Purpose

The purpose of this Security Review Report (SRR) is to provide FSA and MDHEWD with an analysis of the general security and internal controls implemented in the security environment of MDHEWD. The emphasis of this SRR is on the adequacy of the management, operational, and technical security controls implemented to protect the confidentiality, integrity, and availability for information entered, processed, and stored by and within the system. The SRR captures the results of the self-assessment review, including recommendations for correcting any weaknesses or deficiencies in the controls.

1.4 NIST Security Control Set

Table 1: Controls Reviewed

Control Family	Controls Reviewed
ACCESS CONTROL	AC-1, AC-2(1)(2)(3)(4), AC-3, AC-4, AC-5, AC-6(1)(2)(5)(9)(10), AC-7, AC-8, AC-11(1), AC-12, AC-14, AC-17(1)(2)(3)(4), AC-18(1), AC-19(5), AC-20(1)(2), AC-21, AC-22
AUDIT AND ACCOUNTABILITY	AU-1, AU-2(3), AU-3(1), AU-4, AU-5, AU-6(1)(3), AU-7(1), AU-8(1), AU-9(4), AU-11, AU-12
AWARENESS AND TRAINING	AT-1, AT-2(2), AT-3, AT-4
CONFIGURATION MANAGEMENT	CM-1, CM-2(1)(3)(7), CM-3(2), CM-4, CM-5, CM-6, CM-7(1)(2)(4), CM-8(1)(3)(5), CM-9, CM-10, CM-11
CONTINGENCY PLANNING	CP-1, CP-2(1)(3)(8), CP-3, CP-4(1), CP-6(1)(3), CP-7(1)(2)(3), CP-8(1)(2), CP-9(1), CP-10(2)
IDENTIFICATION AND AUTHENTICATION	IA-1, IA-2(1)(2)(3)(8)(11)(12), IA-3, IA-4, IA-5(1)(2)(3)(11), IA-6, IA-7, IA-8(1)(2)(3)(4)
INCIDENT RESPONSE	IR-1, IR-2, IR-3(2), IR-4(1), IR-5, IR-6(1), IR-7(1), IR-8
MAINTENANCE	MA-1, MA-2, MA-3(1)(2), MA-4(2), MA-5, MA-6
MEDIA PROTECTION	MP-1, MP-2, MP-3, MP-4, MP-5(4), MP-6, MP-7(1)
PERSONNEL SECURITY	PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8
PHYSICAL AND ENVIRONMENTAL PROTECTION	PE-1, PE-2, PE-3, PE-4, PE-5, PE-6(1), PE-8, PE-9, PE-10, PE-11, PE-12, PE-13(3), PE-14, PE-15, PE-16, PE-17
PLANNING	PL-1, PL-2(3), PL-4(1), PL-8
RISK ASSESSMENT	RA-1, RA-2, RA-3, RA-5(1)(2)(5)
SECURITY ASSESSMENT AND AUTHORIZATION	CA-1, CA-2(1), CA-3(5), CA-5, CA-6, CA-7(1), CA-9
SYSTEM AND COMMUNICATIONS PROTECTION	SC-1, SC-2, SC-4, SC-5, SC-7(3)(4)(5)(7), SC-8(1), SC-10, SC-12, SC-13, SC-15, SC-17, SC-18, SC-19, SC-20, SC-21, SC-22, SC-23, SC-28, SC-39
SYSTEM AND INFORMATION INTEGRITY	SI-1, SI-2(2), SI-3(1)(2), SI-4(2)(4)(5), SI-5, SI-7(1)(7), SI-8(1)(2), SI-10, SI-11, SI-12, SI-16
SYSTEM AND SERVICES ACQUISITION	SA-1, SA-2, SA-3, SA-4(1)(2)(9)(10), SA-5, SA-8, SA-9(2), SA-10, SA-11

Table 2: Controls Reviewed (Privacy)

Control Family	Controls Reviewed
AUTHORITY AND PURPOSE (Privacy)	AP-1, AP-2
ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (Privacy)	AR-1, AR-2, AR-3, AR-4, AR-5, AR-6, AR-7, AR-8
DATA MINIMIZATION AND RETENTION (Privacy)	DM-1(1), DM-2(1), DM-3(1)
DATA QUALITY AND INTEGRITY (Privacy)	DI-1(1)(2), DI-2(1)
INDIVIDUAL PARTICIPATION AND REDRESS (Privacy)	IP-1(1), IP-2, IP-3, IP-4(1)
SECURITY (Privacy)	SE-1, SE-2
TRANSPARENCY (Privacy)	TR-1(1), TR-2(1), TR-3
USE LIMITATION (Privacy)	UL-1, UL-2

1.5 FSA Team Points of Contact

Table 3: FSA Team Points of Contact lists the members of the FSA Program Management Team for the FY20 GASATRAQ Self-Assessment Review.

Table 3: FSA Team Points of Contact

Name	Role/Responsibility	Contact Information
Daniel Commons	CISO	Daniel.Commons@ed.gov
Theon Dam	GASA Program Manager	Theon.S.Dam@ed.gov Office: +1 (202) 377-3106

1.6 SA Team Points of Contact

Table 4: SA Team Points of Contact lists the members of the SA Team for the FY20 GASATRAQ Self-Assessment Review.

Table 4: SA Team Points of Contact

Name	Role/Responsibility	Contact Information
Mitchell Barth	Program Manager (PM)	MBarth@bluecanopy.com Cell: +1 (703) 217-9523
Phyllis Rhodes	GASA Team Lead	PRhodes@bluecanopy.com Cell: +1 (540) 845-4911
Sarah Krueger (Fletcher)	GASA Deputy Team Lead	SFletcher@bluecanopy.com Cell: +1 (703) 431-6109
Kola Onamade	Lead Assessor	KOnamade@bluecanopy.com Cell: + (240) 460-0633Chris
Christopher Heizer	Support Assessor	CHeizer_CE@bluecanopy.com Cell: + (703) 969-7504

1.7 MDHEWD Points of Contact

Table 5: GA Team Points of Contact lists the members of the MDHEWD Team for the FY20 GASATRAQ Self-Assessment Review.

Table 5: GA Team Points of Contact

Name	Role/Responsibility	Contact Information
Marla Robertson	Director	Marla.Robertson@hewd.mo.gov Cell: + (573) 751-1791
Jeff Ferguson	Secondary Contact	Jeff.Ferguson@oa.mo.gov

2 Analysis Criteria

The SA Team provided the GAs a Draft SRR with an initial rating that was solely established on a rating methodology. This rating was normalized so that each question, security control, or security control family were assessed equitably. Blue Canopy then conducted a Draft SRR Out-brief and follow-up phone interviews with each GA. The SA Team allowed the GAs to submit additional evidence to remediate any of the findings addressed in the Draft SRR. Upon the conclusion of the interviews and additional analysis of the artifacts provided, Blue Canopy subject matter experts (SMEs) made a determination of the GA's rating.

FSA used two (2) metrics for rating criteria:

1. Security control responses
2. Uploaded implementation evidence

Table 6: Analysis Criteria

Effectiveness of the GA Response In Meeting the Security Objective	Strength of Evidence Identified In Meeting the Security Compliance Requirement
Good	• **>= 80%** of the security controls within the control family are Satisfied ○ Good = Assessment evidence satisfactory and/or interview notes indicate security controls are implemented and operating as intended.

Medium	• **>=60% to < 80%** of the security controls within the control family are Satisfied or Partially-Satisfied
	  ○ Medium = Assessment evidence and/or interview notes indicate security controls are mostly implemented and operating as intended.
	• **Rating Override**: If deficiencies were discovered for controls within the control family with a High User Defined Criticality, the rating is determined using the criteria below:
	  ○ High = 1 to 14 Findings

Poor	• **>=30% to < 60%** of the security controls within the control family are Satisfied or Partially-Satisfied
	  ○ Poor = Assessment evidence and/or interview notes indicate security controls are somewhat implemented and operating as intended.
	• **Rating Override**: If deficiencies were discovered for controls within the control family with a High User Defined Criticality, the rating is determined using the criteria below:
	  ○ High = 15 to 19 Findings

Effectiveness of the GA Response In Meeting the Security Objective	Strength of Evidence Identified In Meeting the Security Compliance Requirement

Critical	• **>=0% to < 30%** of the security controls within the control family are Satisfied or Partially-Satisfied
	  ○ Critical = Assessment evidence is not provided and/or interview notes indicate a majority of the security controls are not implemented and operating as intended.
	• **Rating Override**: If deficiencies were discovered for controls within the control family with a High User Defined Criticality, the rating is determined using the criteria below:
	  ○ High = 20 or more Findings

Based on the GA's responses to the Security Self-Assessment questionnaire, the rating methodology, and the results of implementation evidence review, FSA provided a rating for each security control and then calculated an overall rating of Good, Medium, Poor, or Critical for each security control family.

3 Control Family Ratings

FSA calculated a rating based on the GAs responses to the Security Self-Assessment questionnaire. The following results are average ratings for each security control family. The overall rating is an average of all individual NIST control ratings.

Table 7: Control Family Ratings

Control Family Name	2019 Control Family Security Rating	2020 Control Family Security Rating
Access Control (AC)	Medium	Good
Security Awareness and Training (AT)	Good	Good
Auditing and Logging (AU)	Medium	Good
Security Assessments (CA)	Good	Good
Configuration Management (CM)	Medium	Good
Contingency Planning (CP)	Medium	Good
Identification and Authentication (IA)	Good	Good
Incident Response (IR)	Good	Good
Maintenance (MA)	Good	Good
Media Protection (MP)	Good	Good
Physical and Environmental (PE)	Good	Good
Security Planning (PL)	Good	Good
Personnel Security (PS)	Good	Good
Risk Assessment (RA)	Medium	Good
Systems Acquisition (SA)	Good	Good
System and Communications Protection (SC)	Good	Good
System and Information Integrity (SI)	Medium	Good
Privacy (AP, AR, DI, DM, IP, SE, TR, UL)	Good	Good
Overall Rating	**Medium**	**Good**

4 Summary of Findings

The independent analysis of the self-assessment responses identified the following deficient controls for the GA. Detailed weakness information and assessor recommendations are included in Appendix A: MDHEWD Self-Assessment Security Review Analysis Corrective Action Plan (CAP).

Table 8: Summary of Findings

Control Family Name	Finding(s)	Status
Access Control (AC)	AC-11: SESSION LOCK	Remediated
	AC-12: SESSION TERMINATION	Remediated
Auditing and Logging (AU)	AU-2: AUDIT EVENTS	Remediated
	AU-3: CONTENT OF AUDIT RECORDS	Remediated
	AU-6: AUDIT REVIEW, ANALYSIS, AND REPORTING	Remediated
	AU-7: AUDIT REDUCTION AND REPORT GENERATION	Remediated
	AU-8: TIME STAMPS	Remediated
	AU-12: AUDIT GENERATION	Remediated
Security Assessments (CA)	CA-3: SYSTEM INTERCONNECTIONS	Remediated
	CA-5: PLAN OF ACTION AND MILESTONES	Remediated
	CA-7: CONTINUOUS MONITORING	Remediated
	CA-9: INTERNAL SYSTEM CONNECTIONS	Remediated
Configuration Management (CM)	CM-4: SECURITY IMPACT ANALYSIS	Remediated
	CM-5: ACCESS RESTRICTIONS FOR CHANGE	Remediated
	CM-7: LEAST FUNCTIONALITY	Remediated
Systems Acquisition (SA)	SA-1: SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	Remediated
System and Information Integrity (SI)	SI-5: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	Remediated

5 Signature Page

CISO Recommendations:

- Concur with SA Team's GA review
- The GA must:
    - Update all documentation to reflect changes to the information system

Marla Robertson Digitally signed by Marla Robertson
Date: 2020.11.20 15:25:30 -06'00'

Marla Robertson, or designee Date
MDHEWD Signatory

Lisa Ortiz (affiliate) Digitally signed by Lisa Ortiz (affiliate)
Date: 2020.11.20 11:47:58 -05'00'

Mitchell Barth, or designee Date
Blue Canopy - Program Management Office

Theon Dam Date
Federal Student Aid - GASA Program Manager (PM)

Daniel Commons, or designee Date
Director, Enterprise Cybersecurity Group
Federal Student Aid - Chief Information Security Officer (CISO)

6 MDHEWD Finding Details

During the Remediation Window (Monday, August 31 to Friday, November 13, 2020*), GA-MDHEWD submitted additional evidence/ artifacts to the SA Team for review. Upon reviewing the remediation evidence, the SA Team determined that there are no remaining findings for GA-MDHEWD, and the security control requirements have been satisfied.

***NOTE:** Due to unforeseen circumstances, GA-MDHEWD was granted a Remediation Window extension through the end of November 2020 by the FSA CISO. They submitted their remediation evidence prior to the extension end date.

Appendix A: MDHEWD Self-Assessment Security Review Analysis Corrective Action Plan (CAP)

During the Remediation Window (Monday, August 31 to Friday, November 13, 2020*), GA-MDHEWD submitted additional evidence/ artifacts to the SA Team for review. Upon reviewing the remediation evidence, the SA Team determined that there are no remaining findings for GA-MDHEWD, and the security control requirements have been satisfied.

***NOTE:** Due to unforeseen circumstances, GA-MDHEWD was granted a Remediation Window extension through the end of November 2020 by the FSA CISO. They submitted their remediation evidence prior to the extension end date.