Tab 21

Overview of Recent Audit Reports

Coordinating Board for Higher Education
September 16, 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

USDE Information Security Self-Assessment - 2020

Missouri was selected, along with 12 other guaranty agencies, to complete a 2020 Self-Assessment of our 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 185 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 is attached. The report provides an overall rating of DHEWD as "good." There are 21 findings noted. DHEWD has until September 16, 2020 to conduct remediation activities.

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 until November. During the July update call with USDE, DHEWD staff informed USDE of the delay until November. 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. DHEWD supplied evidence that it is conducting scans and resolving the scans on September 7, 2020, but did not provide the actual vulnerability scans themselves. It remains to be seen whether USDE will close the findings without receiving the actual scans.

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 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. A copy of the response is attached. To date, DHEWD has not received a response to its submission.

State Auditor – 2020

The State Auditor will audit the DHEWD loan program, sample some GR funds against the DHEWD internal control plan, and review some other DHEWD federal funds for the CAFR. The State Auditor does not plan to audit the WIOA funds at this time. The State Auditor plans to begin the audit in September of 2020.

NEXT STEPS

DHEWD conducted remediation activities and is waiting for a response from USDE on the Information Security Self-Assessment.

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

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

DHEWD will work with the State Auditor on the upcoming audit of the loan program and other funds.

RECOMMENDATION

This is an information item only.

ATTACHMENTS

A. USDE Self-Assessment Security Review Report 2020-08-26
B. MDHEWD Program Review Report Response 2020-06-01

DEPARTMENT OF
HIGHER EDUCATION &
WORKFORCE DEVELOPMENT

June 1, 2020

Ms. Teresa Napier
Sr. Guarantor and Lender Review Specialist
U.S. Department of Education
Financial Institution Oversight Service – Southern Division
Harwood Center
1999 Bryan Street, Suite 1610
Dallas, TX 75201-6817
Sent via electronic mail to Teresa.Napier@ed.gov

Re: Program Review Report
OPE ID: 99972400 / 729
PRCN: 20194065004

Dear Ms. Napier:

I am writing in response to the U.S. Department of Education review of the Missouri Department of Higher Education and Workforce Development administration of the Federal Family Education Loan (FFEL) Program and the related review report dated March 30, 2020.

The above-referenced report notes a violation of 34 CFR 682.404(j)(4), which provides a prohibition against conflicts - an entity performing any default aversion activities may not perform collection activities on the loan in the event of a default within 3 years of the claim payment date. Please see the enclosed MDHEWD response to the finding.

If you have questions or feedback regarding this response, please contact me at 573-751-1791 or marla.robertson@dhewd.mo.gov. Thank you.

Sincerely,

Marla Robertson

Marla Robertson
Director
Missouri Student Loan Program

Enclosure

Finding: Conflict of Interest Violation

Noncompliance:

MDHEWD contracts with Ascendium Education Solutions, Inc. (Ascendium) for servicing of guaranty activities on behalf of MDHEWD. Under this contract, Ascendium is responsible for default aversion activities and post default collections. In accordance with 34 CFR 682.404(j)(4), if a guaranty agency contracts with an outside entity to perform any default aversion activities, that outside entity may not hold or service the loan; or perform collection activities on the loan in the event of default within 3 years of the claim payment date.

Required Action:

MDHEWD must terminate contracting arrangements that create a conflict of interest and provide the Department with MDHEWD's plan for elimination this conflict of interest and its plan for future default aversion and collections activities.

MDHEWD Response:

Ascendium Education Solutions Inc. is responsible for providing an operational system for MDHEWD guaranty functions. They are also responsible for printing and storing MDHEWD forms. They mail letters requested by MDHEWD and process return mail. Ascendium does perform default aversion assistance activities for delinquent MDHEWD accounts but Ascendium does not perform collection activities for defaulted MDHEWD accounts.

34 CFR 682.404(j)(4) reads…

> *(4) Prohibition against conflicts. If a guaranty agency contracts with an outside entity to perform any default aversion activities, that outside entity may not—*
>
> *(i) Hold or service the loan; or*
>
> *(ii) Perform collection activities on the loan in the event of default within 3 years of the claim payment date.*

Ascendium completes default aversion activities on behalf of MDHEWD. Ascendium does not hold or service the loans in the MDHEWD portfolio. Additionally, Ascendium does not perform collection activities on MDHEWD guaranteed loans that default. All MDHEWD defaulted accounts are collected solely by a third party collection agency or the MDHEWD internal AWG staff as identified by the CAGY field in the Ascendium system. Therefore, MDHEWD respectfully disagrees with the finding and feels there is no conflict of interest. The Ascendium staff that perform default aversion assistance for MDHEWD do not make collection calls or

initiate administrative wage garnishments. Collection agencies under Navient's Master Servicer Agreement perform collection activities. Additional Administrative Wage Garnishment collection activities are performed by internal MDHEWD staff. MDHEWD staff members initiate Notices Prior to Wage Withholding, Orders of Withholding and establish voluntary repayment arrangements for borrowers wishing to avoid garnishment. No collection calls are made by Ascendium staff.

MDHEWD can provide the Department a list of the Ascendium staff that perform default aversion efforts and the MDHEWD staff that perform our internal collections. Additionally, we can provide you screen shots that show the collection agency code a defaulted account is assigned to. Section 3.1.4 of the MDHEWD and Ascendium contract identifies that the contractor's operational services shall comply with all applicable federal and state statutory and regulatory requirements, including any changes or amendment that may be made to those statutes and regulation. In an effort to make the separation more clear going forward we can update our student loan administration services contract to specify compliance with 34 CFR 682.404(j)(4).

MDHEWD was not aware the Department had concerns regarding a conflict of interest. We do not recall any mention of a concern from the Department reviewers during our review conducted at Ascendium's location in July 2019 or during our program review discussions or exit conference calls conducted over the phone in September 2019. Had MDHEWD known the Department reviewers had concerns we would have made a better effort to explain our process. We apologize for any confusion.

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)

Tuesday, August 25, 2020

Version 0.4 (Draft)

Delivered by Blue Canopy Group, LLC | Powered by JACOBS

Document Version Control

Version	Date	Author	Description
0.1	2020-08-17	Blue Canopy Team	Initial version.
0.2	2020-08-19	Blue Canopy Team	Quality Assurance review (Peer).
0.3	2020-08-20	Blue Canopy Team	Quality Assurance review (Team Lead).
0.4	2020-08-26	Blue Canopy Team	Management review.

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.

Appendix A: MDHEWD Self-Assessment Security Review Analysis Corrective Action Plan (CAP) details remediation recommendations, aggregated by control ID, and associated threat levels. This section needs to be completed by the GA no later than Wednesday, September 16, 2020 with planned corrective actions inform FSA of 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.

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

Control Family	Controls Reviewed
ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (Privacy)	AR-1, AR-2, AR-3, AR-4, AR-5, AR-6, AR-7, AR-8
AUTHORITY AND PURPOSE (Privacy)	AP-1, AP-2
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 2: FSA Team Points of Contact lists the members of the FSA Program Management Team for the FY20 GASATRAQ Self-Assessment Review.

Table 2: 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 3: SA Team Points of Contact lists the members of the SA Team for the FY20 GASATRAQ Self-Assessment Review.

Table 3: SA Team Points of Contact

Name	Role/Responsibility	Contact Information
Mitchell Barth	Program Manager (PM)	Mitchell.Barth@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) 460-0633
Christopher Heizer	Support Assessor	CHeizer_CE@bluecanopy.com Cell: + (703) 969-7504

1.7 MDHEWD Points of Contact

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

Table 4: GA Team Points of Contact

Name	Role/Responsibility	Contact Information
Marla Robertson	IT Security Contact	Marla.Robertson@hewd.mo.gov Cell: + (573) 751-1791
Robert Powell	Secondary Contact	Robert.Powell@hewd.mo.gov Cell: + (573) 526-0173

2 Analysis Criteria

The SA Team provide the GAs a Draft SRR with an initial rating that is solely established on a rating methodology. This rating is normalized so that each question, security control, or security control family are assessed equitably. Blue Canopy will then conduct a Draft SRR Out-Brief and follow-up phone interviews with each GA. The SA Team allows 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) will make a determination of the GA's rating.

FSA used two (2) metrics for rating criteria:

1. Security control responses
2. Uploaded implementation evidence

Table 5: 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 6: 2019 Control Family Ratings

Control Family Name	2019 Rating per Security Control Family
Access Control (AC)	Medium
Security Awareness and Training (AT)	Good
Auditing and Logging (AU)	Medium
Security Assessments (CA)	Good
Configuration Management (CM)	Medium
Contingency Planning (CP)	Medium
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)	Medium
Systems Acquisition (SA)	Good
System and Communications Protection (SC)	Good
System and Information Integrity (SI)	Medium
Privacy (AP, AR, DI, DM, IP, SE, TR, UL)	Good
Overall Rating	**Medium**

Table 7: 2020 Control Family Ratings

Control Family Name	Rating per Security Control Family
Access Control (AC)	Good
Security Awareness and Training (AT)	Good
Auditing and Logging (AU)	Poor
Security Assessments (CA)	Poor
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**

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)
Access Control (AC)	AC-11: SESSION LOCK AC-12: SESSION TERMINATION
Audit and Accountability (AU)	AU-2: AUDIT EVENTS AU-3: CONTENT OF AUDIT RECORDS AU-6: AUDIT REVIEW, ANALYSIS, AND REPORTING AU-7: AUDIT REDUCTION AND REPORT GENERATION AU-8: TIME STAMPS AU-12: AUDIT GENERATION
Security Assessment and Authorization (CA)	CA-3: SYSTEM INTERCONNECTIONS CA-5: PLAN OF ACTION AND MILESTONES CA-7: CONTINUOUS MONITORING CA-9: INTERNAL SYSTEM CONNECTIONS
Configuration Management (CM)	CM-4: SECURITY IMPACT ANALYSIS CM-5: ACCESS RESTRICTIONS FOR CHANGE CM-7: LEAST FUNCTIONALITY
Physical and Environmental Protection (PE)	PE-10: EMERGENCY SHUTOFF PE-11: EMERGENCY POWER PE-12: EMERGENCY LIGHTING PE-14: TEMPERATURE AND HUMIDITY CONTROLS PE-15: WATER DAMAGE PROTECTION
System and Services Acquisition (SA)	SA-1: SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
System and Information Integrity (SI)	SI-5: SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

5 Signature Page

CISO Recommendations:

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

Marla Robertson, or designee Date
MDHEWD - Signatory

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

The purpose of this section is to detail the findings discovered before the Remediation Period (Monday, August 31 to Wednesday, September 16, 2020).

6.1 Access Control (AC)

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
AC-11	SESSION LOCK	1. For each information system within the security boundary, does the information system initiate a session lock after a period of inactivity? 2. Does the information system initiate the session lock after?	No evidence was provided specific to this control. To satisfy this control, provide evidence that validates the system has the capability to initiate session lock, and that it is executed after 30 minutes of inactivity (i.e. screenshot(s) from the Active Directory group policy settings which demonstrates the session lock policy).
AC-12	SESSION TERMINATION	1. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, or time-of-day restrictions on information system use. For each information system within the security boundary, does the information system automatically terminate user sessions after a defined conditions or trigger events? 2. Does the information system terminate the user session after?	No evidence was provided specific to this control. To satisfy this control, provide evidence that validates the system has the capability to initiate session termination on user-initiated logical session, and that it is executed after 30 minutes of inactivity or other organization-defined trigger (i.e. screenshot(s) from the Active Directory group policy settings which demonstrates the session termination policy).

6.2 Audit and Accountability (AU)

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
AU-2	AUDIT EVENTS	1. Does the information system capture audit information and if so, is this function operational? 2. Does the information system audit all of the following event types? a) User successful logins, logoffs b) User failed login attempts c) Data viewed d) Data updated e) Data deleted f) Changes in data access g) User accounts created h) User accounts modified 3. The organization reviews the audit records? 4. Does this organization coordinate with other entities to enhance mutual support and guide logging parameter selection? 5. Is there a documented rationale explaining why these logged events will support after-action investigations of security incidents?	The evidence provided is insufficient. The evidence consists of a spreadsheet titled, “MO Last Used List 2nd Quarter 2020” which includes User ID, Last Used (blank if never used), Created, and Username for Great Lakes TSS Confidential Data Usage Information for Missouri Mainframe IDS. This evidence fails to validate any of the implementation requirements for this control. To satisfy this control, provide additional evidence to include sample audit logs (or screenshots of audit logs) and any applicable configuration settings exports for each type of device and application used within the system. Additionally, provide a list of the selected events to be audited within the system, including a rationale for why the current selection is adequate to support the after-the-fact investigation of security incident.
AU-3	CONTENT OF AUDIT RECORDS	1. Do audit records contain the following information: Type of event? When the event occurred? Where the event occurred? The source of the event? Event outcome/end state? Individual or agent associated with the event?	No evidence was provided specific to this control. To satisfy this control, provide evidence that demonstrates the various content included in an audit record (i.e. sample audit logs or screenshots of audit logs).
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	1. The organization reviews the audit records for indications of inappropriate or unusual activity weekly? 2. If yes, are their management level reviews the audit records for indications of inappropriate or unusual activity quarterly?	No evidence was provided specific to this control. To satisfy this control, provide evidence that demonstrates that audit records are reviewed and analyzed to determine if indications of compromise. Additionally, provide evidence which demonstrates the frequency of the reviews and

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
		3. Are automated mechanisms used to support all audit activities below: review? analysis? reporting? 4. Are findings reported to the Security Manager and CIO? 5. Are audit records analyzed and correlated across different repositories to gain situational awareness?	records of recently reported suspicious activities resulting from the review and analysis of audit records.
AU-7	AUDIT REDUCTION AND REPORT GENERATION	1. Does the information system have an audit reduction and report creation capacity? 2. Does that audit report tool support on-demand: audit review? analysis? reporting requirements? 3. Can the information system filter audit records for events of interest, based on any or all of the audit fields? 4. Does the audit report tool prevent: alteration of original contents or alteration of time lines of records?	No evidence was provided specific to this control. To satisfy this control, provide examples of on-demand reports generated by auditing mechanisms and evidence which demonstrates that content or time ordering of audit information used to support the system audit reduction and reporting capability cannot be altered.
AU-8	TIME STAMPS	1. Does the information system apply time stamps to audit records? 2. Are time stamps determined by: Using internal clocks mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT)? 3. Does the information system perform all of the below activities: Compare the internal clocks every 64 seconds with the time.nest.gov time? Synchronize the internal system clocks with the authoritative time source when the time difference exceeds one second?	No evidence was provided specific to this control. To satisfy this control, provide a copy of audit records with a time stamp.
AU-12	AUDIT GENERATION	1. Does the information system provide audit records for the list of auditable events in AU-2 for: all systems which handle confidential	No evidence was provided specific to this control. To satisfy this control, provide sample audit logs (or screenshots of audit logs) and any applicable

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
		information? accept network connections? provide access control? 2. Does the information system allow authorized personnel to select which auditable events are to be captured by specific components? 3. Does the information system generate audit records for all the audit events listed previously?	configuration settings exports for each type of device and application used within the system. Additionally, provide a list of the selected events to be audited within the system, including a rationale for why the current selection is adequate to support the after-the-fact investigation of security incidents.

6.3 Security Assessment and Authorization (CA)

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
CA-3	SYSTEM INTERCONNECTIONS	1. Are connections from the information system to other information systems authorized through the use of Interconnection Security Agreements (ISA)? 2. Are the following documented for each interconnection? a) Interface characteristics b) Security requirements c) Nature of the information communicated 3. Are the ISAs reviewed and updated as needed or when changes are implemented? 4. Is there a policy employed for allowing organization-defined information systems to connect to external information systems? 5. Does the organization implement the one of the following firewall/network access rules for interconnections and network access?	No evidence was provided specific to this control. To satisfy this control, provide ISAs/ MOUs/ other agreement documentation for authorized external systems.
CA-7	CONTINUOUS MONITORING	1. Is there a continuous monitoring strategy in place? 2. Is there a continuous monitoring program? 3. Does the continuous monitoring program include all of the following requirements? a) Establishment of devices and traffic to be monitored b) Establishment of organization-defined frequencies for monitoring and assessments supporting such monitoring c) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy d) Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy	No evidence was provided specific to this control. To satisfy this control, provide evidence demonstrating MDHE has developed a continuous monitoring strategy to include ongoing status monitoring, personnel or roles and a program that includes reporting status with organizational defined frequency.

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
		e) Correlation and analysis of security-related information generated by assessments and monitoring f) Response actions to address results of the analysis of security-related information g) Reporting the security status of organization and the information system to organization-defined personnel or roles at the organized defined frequency	
CA-9	INTERNAL SYSTEM CONNECTIONS	1. Are internal connections agreements authorized to the information system? Example - Non-FSA systems that interconnect with your FSA specific systems within the organization. Are those connections authorized? 2. Are all of following documented for each internal connection? a) Interface characteristics b) Security requirements c) Nature of the information communicated	No evidence was provided specific to this control. To satisfy this control, provide documentation that indicates the approved internal connections with the system. Additionally, provide documentation that indicates the interface characteristics, security requirements, and information communicated for each internal connection used within the system.

6.4 Configuration Management (CM)

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
CM-4	SECURITY IMPACT ANALYSIS	1. Does the organization perform security impact analysis prior to implementation?	The evidence provided is insufficient. The evidence consists of a copy of the Compliance Component System Security Certification and Accreditation Process document. This document fails to address how MDHEWD performs security impact analysis prior to implementation. To fully satisfy this control, provide a list of system changes which have taken place since the assessment of the CM-4 control, as well as a Security Impact Analysis (SIA) report for each said system change.
CM-5	ACCESS RESTRICTIONS FOR CHANGE	1. Are configuration changes protected by physical and logical access restrictions? 2. Which of the following Access Restrictions to Change processes are implemented? a) Access Restrictions are defined b) Access Restrictions are documented c) Access Restrictions are approved	No evidence was provided specific to this control. To satisfy this control, provide evidence that MDHE defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Additionally, provide a list of personnel which are authorized to perform change tasks on the system, mechanisms in place to prevent unauthorized personnel from performing change tasks, and approval process for granting authorization to perform change requests.
CM-7	LEAST FUNCTIONALITY	1. Does the information system provide the least functionality to meet operational needs? 2. Does the information system prohibit or restrict ports, protocols, and services for all of the following areas: Software Systems? System Data? Systems Services? 3. Does the organization perform all of the following requirements: Review the information system to identify unnecessary	No evidence was provided specific to this control. Provide evidence demonstrating that MDHE defines and prohibits/ restricts functions, ports, protocols, and services. Additionally, provide configuration settings/ policy settings illustrating that services or ports that are not needed are disabled.

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
		and/or non-secure functions, ports, protocols, and services? Disable unnecessary or non-secure software systems access, data access, and system services? 4. Does the information system prevent program execution in accordance with the security plan? 5. Does the organization perform all of the following requirements: Identify software programs not authorized to execute on the information system? Employ a deny-all, allow by exception policy to prohibit the execution of unauthorized software on the information system? Review and update a list of unauthorized software programs?	

6.5 Physical and Environmental Protection (PE)

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
PE-10	EMERGENCY SHUTOFF	1. Is the capability of shutting off power to the information system or individual system components provided in emergency situations? 2. Are emergency shutoff switches or devices placed according to the organization-defined location by information system or system component to facilitate safe and easy access for personnel? 3. Is emergency power shutoff capability protected from unauthorized activation?	No evidence was provided specific to this control. To satisfy this control, provide a picture of the emergency shutoff switch/ device.
PE-11	EMERGENCY POWER	1. Is a short-term uninterruptible power supply provided to facilitate [an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss?	No evidence was provided specific to this control. To satisfy this control, provide a picture of the UPS.
PE-12	EMERGENCY LIGHTING	1. Is an automatic emergency lighting employed and maintained for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility?	No evidence was provided specific to this control. To satisfy this control, provide a picture of the automated emergency lighting in place for MDHEWD (i.e. Emergency Exit signs and evacuation routes).
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	1. Are temperature and humidity levels maintained within the facility where the information system resides at organization-defined acceptable levels?	No evidence was provided specific to this control. To satisfy this control, provide documentation that addresses the organization-defined acceptable temperature and humidity levels as well as a picture of the levels meeting that threshold. Additionally, provide evidence demonstrating these levels are being monitored, and the frequency at which they are being monitored.
PE-15	WATER DAMAGE PROTECTION	1. Is the information system protected from damage resulting from water leakage by	No evidence was provided specific to this control.

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
		providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel?	To satisfy this control, provide a picture of the master shutoff or isolation valves that are accessible to key personnel. Additionally, provide evidence demonstrating that the devices are working properly.

6.6 System and Services Acquisition (SA)

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	1. Which of the following requirements are addressed by the system and services acquisition policy? a) Scope b) Roles and Responsibilities c) Management Commitment d) Organizational Coordination e) Compliance Measures	The evidence provided is insufficient. The evidence consists of a copy of the Technology Area - System Life Cycle Security document. This document fails to address the the purpose, scope, roles and responsibilities, management commitment, organizational coordination, and compliance measures required of a System and Services Acquisitions Policy. To fully satisfy this control, ensure the document provided specifically addresses the purpose, scope, roles and responsibilities, management commitment, organizational coordination, and compliance measures for system and services acquisitions within the MDHEWD system.

6.7 System and Information Integrity (SI)

Failed Control	Failed Control Title	Failed Question(s)	Assessor Comments
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	1. Does the organization receive alerts for third-party vendors on threat intelligence and security alerts?	No evidence was provided specific to this control. To satisfy this control, provide evidence demonstrating security alerts, advisories, and directives from entities such as Department of Homeland Security (DHS), Federal Bureau of Investigations (FBI), Department of Education (ED) or other participating agencies are received. Furthermore, provided Evidence of disseminating aforementioned security alerts to appropriate management (e.g. email).

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

Due to FSA: Wednesday, September 16, 2020

Purpose: This CAP outlines the Self-Assessment Security Review findings resulting from responses of partially satisfied or not satisfied security control implementation and the GA's plan to address each finding.

The GA is responsible for completing Appendix A by populating the following columns for each of the listed findings: *Agency Concurs, Corrective Actions(s), Status,* and *ECD.* The GA should provide enough information for FSA and the SA Team to understand the GA's plan to correct the findings, if remediation is currently in progress, if compensating controls are in place or planned, and/or if the GA plans to accept the risk (justification must be provided)

- ***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
  - Very Low
- ***Agency Concurs with Recommended Remediation***:
  - Concur
  - Does Not Concur
    - For the Corrective Actions, the compensating controls or risk acceptance approach must be stated.
- ***Status***: Status of the finding remediation/mitigation effort
  - **NS** = Not Started
  - **U** = Underway
  - **C** = Completed
  - **RA =** Risk Acceptance
- ***Estimated Completion Date (ECD)****:* Expected date the finding will be remediated; include any planned milestones

A.1 Access Control (AC)

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
AC-11	No evidence was provided specific to this control.	To satisfy this control, provide evidence that validates the system has the capability to initiate session lock, and that it is executed after 30 minutes of inactivity (i.e. screenshot(s) from the Active Directory group policy settings which demonstrates the session lock policy).	Moderate				
AC-12	No evidence was provided specific to this control.	To satisfy this control, provide evidence that validates the system has the capability to initiate session termination on user-initiated logical session, and that it is executed after 30 minutes of inactivity or other organization-defined trigger (i.e. screenshot(s) from the Active Directory group policy settings which demonstrates the session termination policy).	Moderate				

A.2 Audit and Accountability (AU)

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
AU-2	The evidence provided is insufficient. The evidence consists of a spreadsheet titled, “MO Last Used List 2nd Quarter 2020” which includes User ID, Last Used (blank if never used), Created, and Username for Great Lakes TSS Confidential Data Usage Information for Missouri Mainframe IDS. This evidence fails to validate any of the implementation requirements for this control.	To satisfy this control, provide additional evidence to include sample audit logs (or screenshots of audit logs) and any applicable configuration settings exports for each type of device and application used within the system. Additionally, provide a list of the selected events to be audited within the system, including a rationale for why the current selection is adequate to support the after-the-fact investigation of security incident.	Moderate				
AU-3	No evidence was provided specific to this control.	To satisfy this control, provide evidence that demonstrates the various content included in an audit record (i.e. sample audit logs or screenshots of audit logs).	Moderate				
AU-6	No evidence was provided specific to this control.	To satisfy this control, provide evidence that demonstrates that audit	Moderate				

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
		records are reviewed and analyzed to determine if indications of compromise. Additionally, provide evidence which demonstrates the frequency of the reviews and records of recently reported suspicious activities resulting from the review and analysis of audit records.					
AU-7	No evidence was provided specific to this control.	To satisfy this control, provide examples of on-demand reports generated by auditing mechanisms and evidence which demonstrates that content or time ordering of audit information used to support the system audit reduction and reporting capability cannot be altered.	Moderate				
AU-8	No evidence was provided specific to this control.	To satisfy this control, provide a copy of audit records with a time stamp.	Moderate				

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
AU-12	No evidence was provided specific to this control.	To satisfy this control, provide sample audit logs (or screenshots of audit logs) and any applicable configuration settings exports for each type of device and application used within the system. Additionally, provide a list of the selected events to be audited within the system, including a rationale for why the current selection is adequate to support the after-the-fact investigation of security incidents.	Moderate				

A.3 Security Assessment and Authorization (CA)

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
CA-3	No evidence was provided specific to this control.	To satisfy this control, provide ISAs/ MOUs/ other agreement documentation for authorized external systems.	Low				
CA-7	No evidence was provided specific to this control.	To satisfy this control, provide evidence demonstrating MDHE has developed a continuous monitoring strategy to include ongoing status monitoring, personnel or roles and a program that includes reporting status with organizational defined frequency.	Low				
CA-9	No evidence was provided specific to this control.	To satisfy this control, provide documentation that indicates the approved internal connections with the system. Additionally, provide documentation that indicates the interface characteristics, security requirements, and information communicated for each	Low				

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
		internal connection used within the system.					

A.4 Configuration Management (CM)

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
CM-4	The evidence provided is insufficient. The evidence consists of a copy of the Compliance Component System Security Certification and Accreditation Process document. This document fails to address how MDHEWD performs security impact analysis prior to implementation.	To fully satisfy this control, provide a list of system changes which have taken place since the assessment of the CM-4 control, as well as a Security Impact Analysis (SIA) report for each said system change.	Moderate				
CM-5	No evidence was provided specific to this control.	To satisfy this control, provide evidence that MDHE defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Additionally, provide a list of personnel which are authorized to perform change tasks on the system, mechanisms in place to prevent unauthorized personnel from performing change tasks, and approval process for granting	Moderate				

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
		authorization to perform change requests.					
CM-7	No evidence was provided specific to this control.	Provide evidence demonstrating that MDHE defines and prohibits/ restricts functions, ports, protocols, and services. Additionally, provide configuration settings/ policy settings illustrating that services or ports that are not needed are disabled.	Moderate				

A.5 Physical and Environmental Protection (PE)

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
PE-10	No evidence was provided specific to this control.	To satisfy this control, provide a picture of the emergency shutoff switch/ device.	Low				
PE-11	No evidence was provided specific to this control.	To satisfy this control, provide a picture of the UPS.	Low				
PE-12	No evidence was provided specific to this control.	To satisfy this control, provide a picture of the automated emergency lighting in place for MDHEWD (i.e. Emergency Exit signs and evacuation routes).	Low				
PE-14	No evidence was provided specific to this control.	To satisfy this control, provide documentation that addresses the organization-defined acceptable temperature and humidity levels as well as a picture of the levels meeting that threshold. Additionally, provide evidence demonstrating these levels are being monitored, and the frequency at which they are being monitored.	Low				

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
PE-15	No evidence was provided specific to this control.	To satisfy this control, provide a picture of the master shutoff or isolation valves that are accessible to key personnel. Additionally, provide evidence demonstrating that the devices are working properly.	Low				

A.6 System and Services Acquisition (SA)

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
SA-1	The evidence provided is insufficient. The evidence consists of a copy of the Technology Area - System Life Cycle Security document. This document fails to address the the purpose, scope, roles and responsibilities, management commitment, organizational coordination, and compliance measures required of a System and Services Acquisitions Policy.	To fully satisfy this control, ensure the document provided specifically addresses the purpose, scope, roles and responsibilities, management commitment, organizational coordination, and compliance measures for system and services acquisitions within the MDHEWD system.	Low				

A.7 System and Information Integrity (SI)

Failed Control	Weakness(es)	Recommendation(s)	Threat Level	Agency Concurs	Corrective Action(s)	Status	Estimated Completion Date (ECD)
SI-5	No evidence was provided specific to this control.	To satisfy this control, provide evidence demonstrating security alerts, advisories, and directives from entities such as Department of Homeland Security (DHS), Federal Bureau of Investigations (FBI), Department of Education (ED) or other participating agencies are received. Furthermore, provided Evidence of disseminating aforementioned security alerts to appropriate management (e.g. email).	Moderate				