Tab 29

Overview of Recent Audit Reports

Coordinating Board for Higher Education
December 11, 2019

BACKGROUND

MDHEWD 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) 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

DHEWD received the final report from the current-year USDE Information Security Controls audit. There are 23 findings. DWEWD staff are now working with OA-ITSD staff on resolving the findings.

USDE conducted its Program Review of DHEWD's Student Loan Program loan servicer, Ascendium Education, on-site at Ascendium, July 16-19, 2019. During the exit conference there were no findings identified. DHEWD is still waiting on the final audit report.

At the September board meeting, DHEWD staff had started working with the SAO on the fiscal year 2019 SEFA. The SAO uses this audit as part of the CAFR. DHEWD staff are still working with the SAO to provide all needed information.

RubinBrown conducted its interim field work and is presenting to the board today.

NEXT STEPS

MDHEWD will continue to provide the CBHE with an update on the status of the 23 remaining findings related to the USDE's Information Security Audit at future public meetings. A copy of the USDE's Final Information Security Audit is attached.

MDHEWD will provide the CBHE with a copy of the Student Loan Program audit of Ascendium when available.

MDHEWD will continue to work with the State Auditor's Office while they conduct their audit and provide an update at the next public meeting.

RECOMMENDATION

This is an information item only.

ATTACHMENT

- USDE Final Information Security Audit

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

PROUD SPONSOR of the AMERICAN MIND®

Missouri Department of Higher Education (GA-MDHE)
Guaranty Agency Review 2019
Security Review Report (SRR)

2019-09-13

Version 1.0 FINAL

Delivered by Blue Canopy Group, LLC | Powered by JACOBS

CONTROLLED UNCLASSIFIED INFORMATION

Document Version Control

This page summarizes the change history for the document.

VERSION	DATE	AUTHOR	DESCRIPTION
0.1	2019-07-12	Blue Canopy Team	Initial document preparation.
0.2	2019-07-18	Blue Canopy Team	Released for FSA / GA-MDHE review.
0.3	2019-08-26	Blue Canopy Team	Released for QA.
0.4	2019-08-28	Blue Canopy Team	Released to GA-MDHE for updates to Appendix A.
0.5	2019-09-06	MDHE Team	Updated Appendix A.
1.0 FINAL	2019-09-13	Blue Canopy Team	Final SRR delivered to FSA and GA-MDHE.

Table of Contents

Section 1. 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 ("SA Team") conducted an independent Security Control Review on the Missouri Department of Higher Education (GA-MDHE) information system.

1.1. Security Control Review

The SA Team performed control testing using National Institute of Standards (NIST) Special Publication 800-53A Revision 4 test cases, using the FSA critical (NIST) control baseline, to evaluate the information system for compliance with NIST. The SA Team performed an onsite review at 205 Jefferson Street, Jefferson City, MO 65201 from Tuesday, May 21, 2019 to Wednesday, May 22, 2019. Follow-up interviews were conducted on Wednesday, May 29, 2019. The findings associated with the controls evaluated are listed below. The SA Team can provide the Security Requirements Traceability Matrix (SRTM) upon request, which provides more detail into how the control compliance was determined. This report also provides recommendations for how to remediate these findings.

1.2. Scanning Activities

During the security control review, the SA Team observed vulnerability scanning activities conducted by GA-MDHE personnel Tuesday, May 21, 2019 - Wednesday, May 22, 2019 against the information system at the operating system, database, web, and network device layers. In addition, the GA-MDHE personnel provided vulnerability scan results while onsite at FSA on August 21, 2019 – August 22, 2019. This report documents the findings of the vulnerability scanning and other security assessment activities. The raw results were analyzed to reduce false positives as well as aggregate and group vulnerabilities by similar risk categorizations. This provides the stakeholders with actionable recommendations in order to remediate vulnerabilities and reduce risk.

1.3. FSA Points of Contact

Table 1: FSA Points of Contact lists the members of the FSA GA Program Management Team for the 2019 GA Onsite Review.

Table 1: FSA Points of Contact

NAME	ROLE/RESPONSIBILITY	CONTACT INFORMATION
Andy Newton	GASA Program Manager	Andy.Newton@ed.gov Phone: (202) 377-4426
Theon Dam	GASA Project Manager	Theon.Dam@ed.gov Cell: (703) 864-2274

1.4. SA Team Points of Contact

Table 2: SA Team Points of Contact lists the members of the SA Team for the 2019 Onsite Review.

Table 2: SA Team Points of Contact

NAME	ROLE/RESPONSIBILITY	CONTACT INFORMATION
Jonathan Edwards	Program Manager	JEdwards@bluecanopy.com Cell: (202) 368-7177
Aaron Shortridge	GASA Team Lead	AShortridge@bluecanopy.com Cell: (206) 724-7992
Sarah Fletcher	GASA Deputy Team Lead	SFletcher@bluecanopy.com Cell: (703) 431-6109
Thomas Perry	Security Control Assessor – Lead	TPerry@bluecanopy.com Cell: (703) 439-4812
Donald Chinnis	Security Control Assessor – Support	DChinnis@bluecanopy.com Cell: (843) 647-8318
Mannal Bakhsh	Security Control Assessor – Support	MBakhsh@bluecanopy.com Cell: (202) 510-7249
David Petersen	Vulnerability Scanning Analysis (VSA) Team Lead	DPetersen2@bluecanopy.com Cell: (571) 332-5105

1.5. GA-MDHE Points of Contact

Table 3: GA Points of Contact lists the GA-MDHE points of contact for the 2019 Onsite Review.

Table 3: GA Points of Contact

NAME	ROLE/RESPONSIBILITY	CONTACT INFORMATION
Marla Robertson	MDHE Assistant Commissioner, Missouri Student Loan Group	Marla.Robertson@dhe.mo.gov
Robert Powell	MDHE Senior Associate for Information Security	Robert.Powell@dhe.mo.gov Phone: (573) 526-0173
Jeff Ferguson	Office of Administration – Information Technology Services Division (ITSD), Office of Cyber Security	Jeff.Ferguson@oa.mo.gov
Pamela Keep	OA-ITSD, Client Service Manager (CSM)	Pamela.Keep@oa.mo.gov

Section 2. Executive Summary

The purpose of this Security Review Report (SRR) is to provide FSA and GA-MDHE with an analysis of the general security and internal controls implemented in the security environment of GA-MDHE. 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 security control review, including recommendations for correcting any weaknesses or deficiencies in the controls. All applicable documentation is included in the Security Review package.

The overall business impact on FSA and the recommendations of Blue Canopy are presented in the SRR. Vulnerabilities are arranged in order of business impact, with the highest impact issues appearing first.

Section 4.3: Remediation Recommendations details remediation recommendations, aggregated by finding ID. Each entry contains a finding ID listing all affected assets. Additional analysis is performed to identify:

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

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

2.1. Scan Statistics

GA-MDHE personnel conducted the vulnerability scans (no compliance scans were performed) on Thursday, May 2, 2019, and provided results to the SA Team on Tuesday, May 21, 2019.

- **Scans Completed:** Operating Systems
- **Targets Scanned:** 28
- **Individual Findings Discovered:** 288
- **Total Aggregated Findings:** 2

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

While GA-MDHE came onsite to FSA on Wednesday, August 21, 2019 – Thursday, August 22, 2019, the SA Team did not receive updated vulnerability scans that met FSA's scanning requirements documented in the "Guaranty Agency Security Assessment (GASA) scanning and security control review requirements" document. Therefore, only the May 2019 scans could be leveraged for purposes of the assessment. Although there is evidence GA-MDHE is performing vulnerability scanning, there is no evidence that they are creating reports from these vulnerability scans and acting to remediate identified findings.

2.2. Scan Finding Analysis

Although GA-MDHE provided vulnerability scans for viewing while Blue Canopy was onsite in May 2019, GA-MDHE did not permit Blue Canopy to map unique asset ID's (e.g. IP addresses, hostnames) to discovered vulnerabilities. As a work-around, Blue Canopy proposed a method to track the remediation of these vulnerabilities to assets to allow GA-MDHE the opportunity to provide off-site re-scans during the remediation window, without revealing sensitive data.

Alternatively, GA-MDHE and FSA agreed to participate in a second on-site visit, at the FSA offices in Washington, DC, on Wednesday, August 21, 2019 – Thursday, August 22, 2019. During this onsite visit, remediation evidence was analyzed and one-on-one interviews were conducted. During the SA Team's analysis, it was determined that the remediation scans submitted by GA-MDHE did not meet GASA Scanning and Security Control Review Requirements. As a result, the original finding counts, noted while onsite and listed in Section 2.1 (Scan Statistics), remain the same for the final report.

Section 3. Third Party / External Vendor Security Summary

The SA Team analyzed Evidence Request List (ERL) 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 GA-MDHE is fully satisfying these NIST security control requirements of overseeing third party and external entities as they pertain to “Use of External Information Systems”, “Third-Party Personnel Security” and “External Information System Services.” Please see the GA-MDHE SRTM for the complete testing results of these controls.

Ascendium is the only known third party servicer used by GA-MDHE at this time.

Section 4. Findings Summary

4.1. Analysis Criteria

The Guaranty Agencies (GAs) were first provided a draft Preliminary Findings Report (PFR) 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. FSA then conducted in-person and follow-up phone interviews with each GA. Upon the conclusion of the interviews, FSA subject matter experts (SMEs) made a subjective determination of the GA's rating, taking into consideration the interview feedback.

Rating criteria are based on the following two metrics:

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

EFFECTIVENESS OF 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 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 Findings

Based on the GA's responses to the ERL that was submitted, the rating 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.

4.2. Control Family Scores (2018 vs 2019)

Control Family Name	2018 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	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**

4.3. Remediation Recommendations

To ensure that all control families achieve a compliance rating of “Good”, this section provides high-level recommendations for those control families that received a rating lower than “Good”.

- **Access Control (AC)** – Develop and implement an access control strategy ensuring only authorized devices/persons have appropriate access in accordance with business needs. The access control strategy should cover physical and logical access.
- **Audit and Accountability (AU)** - Create, protect, review, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized, or inappropriate information system activity.
- **Configuration Management (CM)** – Document, review and update, and test established configuration settings, with approved deviations at organizationally-defined frequency. Documented baselines, settings and deviations should be protected from unauthorized disclosure.
- **Contingency Planning (CP)** – Document, review, update and implement a contingency plan which includes daily user, system, and documentation level backup at frequency consistent with recovery time and recovery point objectives. Ensure that all backups are protected utilizing technical and/or physical mechanisms.
- **Risk Assessment (RA)** - Remediate all vulnerabilities within defined frequencies that are commensurate with the level of risk the vulnerabilities present, establish, and implement a Vulnerability Management Plan that outlines policy to conduct and review not only Vulnerability, but also Compliance scans at the organizationally-defined frequency with all organizationally-defined personnel or roles.
- **System and Communications Protection (SC)** – Develop, review, update, and implement a system and communications protection strategy which monitors and controls communications at all boundaries (internal and external) at the organizationally-defined frequency. Ensure subnetworks are implemented for publicly accessible system components separated, physically and logically, from internal organizational networks, and protects GA-MDHE information both in-transit and at-rest.
- **System and Information Integrity (SI)** – Develop, review, update, and implement policies and procedures to include hardware and software process isolation within system at the organizationally-defined frequency. Conduct vulnerability scans, development remediation plans and track remediation until closed at documented organizationally-defined risk level priority. Document and implement malicious code protection mechanisms. Ensure that anti-virus agents are implemented on all components and remain up-to-date with latest software updates and signatures.

Section 5. Signature Page

CISO Recommendations:

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

_____ _____

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

Date

Section 6. Preliminary Findings

6.1. Known Findings

The purpose of section 6.1 is to identify Open Corrective Action Plan (CAP) items resulting from the 2018 Onsite Security Review. All Open CAP findings are to be submitted for review/closure to the FSA Plan of Actions & Milestones (POA&M) Team.

6.1.1. Multiple Vulnerabilities Found (RA-5)

NIST SP 800-53 Control: RA-5	**Type:** Corrective Action	**Risk: High**
Affected Asset(s): 1604 Vulnerabilities Discovered		
Status: Pre-Existing CAP **Estimated Completion Date (ECD):** 9/4/2019		
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 GA-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 commensurate with the level of risk the vulnerabilities present.		
Stakeholder Discussion: Discussed this open CAP during the Program Overview and Recommendations Presentation on May 21, 2019. GA-MDHE to send update to FSA GA Management and the FSA POA&M Team for closure.		

6.2. Findings Requiring Discussion

The purpose of this section is to identify findings discovered from the security control review. The following is a list of discovered findings, ordered with the highest impact issues appearing first.

6.2.1. Multiple Vulnerabilities Found (RA-5)

NIST SP 800-53 Control: RA-5	**Type:** Corrective Action	**Risk: High**
Affected Asset(s): RA-5: Vulnerability Scanning		
Status: Additional Analysis Required		
Finding Description: Security Control Assessment (SCA) Finding: 'Multiple Vulnerabilities Found (RA-5)' Affected Asset(s): RA-5: Vulnerability Scanning Instance Detail: 288 Total vulnerabilities were detected for GA-MDHE. Please see breakdown below: • High: 36 • Medium: 200 • Low: 52		
Threat Description: Numerous technical vulnerabilities exist, including lack of evidence provided for patches, misconfigured parameters and unhardened hosts.		
Recommendation: Remediate all vulnerabilities within defined frequencies that commensurate with the level of risk the vulnerabilities present.		

6.2.2. No Evidence provided for FLAW REMEDIATION (SI-2)

NIST SP 800-53 Control: SI-2	**Type:** Corrective Action	**Risk: High**

Affected Asset(s):
SI-2: FLAW REMEDIATION

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for FLAW REMEDIATION (SI-2)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE SI-2.a, b, c, d)
Provide evidence which demonstrates GA-MDHE conducts vulnerability scanning, creates reports based on findings discovered during vulnerability scanning, and corrects vulnerabilities. For example, change tickets and scan reports.

SA Team Comments: Although GA-MDHE is conducting monthly vulnerability scanning, there is no evidence provided to demonstrate GA-MDHE creates reports based on findings discovered during vulnerability scanning, and corrects vulnerabilities.

6.2.3. No Security Configuration Checklists Used to Determine Configuration Settings (CM-6)

NIST SP 800-53 Control: CM-6	**Type:** Corrective Action	**Risk: Medium**
Affected Asset(s): CM-6: CONFIGURATION SETTINGS		
Status: Additional Analysis Required		
Finding Description: Security Control Assessment (SCA) Finding: 'No Security Configuration Checklists Used to Determine Configuration Settings (CM-6)'		
Threat Description: Without using secure configurations, the organization may be overlooking best practices or critical security flaws that could leave the organization susceptible to malicious attacks.		
Recommendation: Use an established security configuration checklist to ensure that products employed within the information system reflect the most restrictive mode consistent with operational requirements (e.g. DISA STIGS, CIS).		

6.2.4. Insufficient Evidence provided for ACCESS CONTROL POLICY AND PROCEDURES (AC-1)

NIST SP 800-53 Control: AC-1	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AC-1: ACCESS CONTROL POLICY AND PROCEDURES

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'Insufficient Evidence provided for ACCESS CONTROL POLICY AND PROCEDURES (AC-1)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AC-1.a, b)
1) Document the GA-MDHE Access Control Policy document. Provide evidence demonstrating the GA-MDHE Access Control Policy has been provided to the organization-defined roles. Provide evidence which confirms that the procedures have been reviewed and updated by GA-MDHE with the organization-defined frequency.

SA Team Comments: Evidence provided does not demonstrate policy addresses all control requirements, and dissemination of policy and procedures to organization-defined personnel or roles. The policy shall include the process for creating, enabling, modifying, disabling, and removing GA-MDHE accounts. The policy shall include the approval process for an GA-MDHE system account (e.g. background investigation, access request submitted by Office Manager, process of requesting new user account from ITSD, and assigning individual access permissions depending on individual's role and responsibility, security group requirements, etc.). Also include policy for conducting GA-MDHE system account monitoring and how often it is conducted. Policy should address separation of duties, least privilege, unsuccessful logon attempts, session termination, etc.

6.2.5. Insufficient Evidence provided for ACCOUNT MANAGEMENT (AC-2)

NIST SP 800-53 Control: AC-2	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AC-2: ACCOUNT MANAGEMENT

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'Insufficient Evidence provided for ACCOUNT MANAGEMENT (AC-2)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AC-2.a, b, c, d, e, f, g, h, I, j, k)
Provide evidence which documents the types of accounts used within the GA-MDHE information system (standard user, privileged user, system accounts, service accounts, shared accounts, temporary or emergency accounts), including the business function met by each type of account. Provide evidence which documents the individual or role responsible for managing each type of account used within the system.

SA Team Comments: Evidence does not demonstrate the types of accounts used within the GA-MDHE information system, including business function for each. Create a roles and responsibilities matrix table listing the different types of GA-MDHE system accounts (standard user, privileged users, Onbase scanner user, System Administrator, Manager, etc.). Include the assignment of GA-MDHE account managers for information system accounts. Document the established membership conditions for each group and/or role used within the system. If shared or group accounts are used, then provide documentation which defines the process for reissuing shared/group credentials when the membership of the group or users of the shared account changes.

6.2.6. Insufficient Evidence provided for ACCESS ENFORCEMENT (AC-3)

NIST SP 800-53 Control: AC-3	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AC-3: ACCESS ENFORCEMENT

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'Insufficient Evidence provided for Evidence for ACCESS ENFORCEMENT (AC-3)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AC-3)
1) Provide documentation which defines the roles and permissions associated with each role used within the system. Provide screenshots which show the effective permissions of standard user accounts, privileged user accounts, and other application accounts which are used within the system.

SA Team Comments: No evidence provided demonstrating the effective permissions of standard user accounts, privileged user accounts, and other application accounts which are used within the system. Provide evidence documented for GA-MDHE AC-2.a. Create a roles and responsibilities matrix table listing the different types of GA-MDHE system accounts (standard user, privileged users, Onbase scanner user, System Administrator, Manager, etc.). Document the conditions for group and role membership.

6.2.7. Insufficient Evidence provided for INFORMATION FLOW ENFORCEMENT (AC-4)

NIST SP 800-53 Control: AC-4	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AC-4: INFORMATION FLOW ENFORCEMENT

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'Insufficient Evidence provided for INFORMATION FLOW ENFORCEMENT (AC-4)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AC-4)
1) Provide configuration files for network devices used within the system which control the flow of information within the system (firewalls, web filtering, VPN, IDS, routers, switches, etc.). Provide screenshots of dashboards, configuration settings, access control lists, and logs which demonstrate how the system controls the flow of information traffic.

SA Team Comments: Evidence provided for the Palo Alto firewall was not for the GA-MDHE servers IP addresses. Provide screen shot for Palo Alto content filtering for GA-MDHE, .129 subnet.

6.2.8. Insufficient Evidence provided for SEPARATION OF DUTIES (AC-5)

NIST SP 800-53 Control: AC-5	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AC-5: SEPARATION OF DUTIES

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'Insufficient Evidence provided for SEPARATION OF DUTIES (AC-5)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AC-5.a)
1) Provide evidence which demonstrates how the system separates privileges and responsibilities within the system (ex. Roles and Responsibilities Matrix). Provide screenshots of permissions used within the system to demonstrate the separation of duties implemented within the system.

SA Team Comments: Evidence does not demonstrate how the system separates privileges and responsibilities (ex. Roles and Responsibilities Matrix). Provide evidence documented for GA-MDHE AC-2.a. Create a roles and responsibilities matrix table listing the different types of GA-MDHE system accounts (standard user, privileged users, Onbase scanner user, System Administrator, Manager, etc.). Document the conditions for group and role membership.

6.2.9. Insufficient Evidence provided for LEAST PRIVILEGE (AC-6)

NIST SP 800-53 Control: AC-6	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AC-6: LEAST PRIVILEGE

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'Insufficient Evidence provided for LEAST PRIVILEGE (AC-6)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AC-6)
Provide a copy of the Roles and Responsibilities Matrix (or equivalent documentation) to demonstrate that permissions for users and processes acting on behalf of users are only provided with permissions and access necessary to perform their job function.

SA Team Comments: No evidence was provided demonstrating the Roles and Responsibilities that permissions for users and processes acting on behalf of users are only provided with permissions and access necessary to perform job function. Create a roles and responsibilities matrix table listing the different types of GA-MDHE system accounts (standard user, privileged users, Onbase scanner user, System Administrator, Manager, etc.). Document the conditions for group and role membership.

6.2.10. No Evidence provided for SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES (AT-1)

NIST SP 800-53 Control: AT-1	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AT-1: SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES (AT-1)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AT-1.a, b)
Document a GA-MDHE Security Awareness and Training Policy and procedures, then provide evidence which confirms that the policy has been reviewed and updated by GA-MDHE with the organization-defined frequency.

SA Team Comments: No evidence provided to demonstrate reviewing and updating of Security Awareness and Training Policy and Procedures. Security Awareness training policy should document how often the training is provided to GA-MDHE employees; if role-based security training is provided to users who have a security/sensitive role, and that security training records are documented and maintained.

6.2.11. No Evidence provided for AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES (AU-1)

NIST SP 800-53 Control: AU-1	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AU-1: AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES (AU-1)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AU-1.a, b)
Document a GA-MDHE Audit and Accountability Policy and Procedures, then provide evidence which confirms that the policy has been reviewed and updated by GA-MDHE with the organization-defined frequency.

SA Team Comments: No evidence provided to demonstrate reviewing and updating of Audit and Accountability Policy and Procedures. Document and draft an audit and accountability policy that addresses GA-MDHE auditing and logging requirements expected from ITSD; what type of events should be audited and logged; the personnel or roles allowed to select these auditable events; how often audit logs should be received from ITSD (weekly, monthly, quarterly), and how ITSD should alert GA-MDHE to certain security incidents/ suspicious activity.

6.2.12. No Evidence provided for AUDIT EVENTS (AU-2)

NIST SP 800-53 Control: AU-2	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AU-2: AUDIT EVENTS

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for AUDIT EVENTS (AU-2)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AU-2.a, b, c)
Provide a list of the selected events to be audited within the system, 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 (Operating System, Database, Active Directory, Exchange, Onbase database, etc.).

SA Team Comments: Evidence provided was lacking to demonstrate list of auditable events and sampling of audit logs (or screenshots of audit logs) from the servers and applications used within the system (Operating System, Database, Active Directory, Exchange, Onbase scanner, etc.). GA-MDHE needs to document and instruct ITSD on the type of events from users which will alert GA-MDHE of suspicious activity.

6.2.13. No Evidence provided for CONTENT OF AUDIT RECORDS (AU-3)

NIST SP 800-53 Control: AU-3	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AU-3: CONTENT OF AUDIT RECORDS

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for CONTENT OF AUDIT RECORDS (AU-3)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AU-3)
Please see the artifacts requested for AU-2.a for details.

SA Team Comments: No evidence provided to demonstrate the content of audit records including: the type of event; when the event occurred; where the event occurred; the source of the event; the outcome of the event, and the identity of any individuals or subjects associated with the event.

6.2.14. No Evidence provided for AUDIT REVIEW, ANALYSIS, AND REPORTING (AU-6)

NIST SP 800-53 Control: AU-6	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
AU-6: AUDIT REVIEW, ANALYSIS, AND REPORTING

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for AUDIT REVIEW, ANALYSIS, AND REPORTING (AU-6)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE AU-6.a)
1) Provide evidence which demonstrates that audit records are reviewed and analyzed to determine if indications of compromise (or other organization-defined inappropriate or unusual activities) have occurred.

SA Team Comments: No evidence provided to demonstrate that audit records are reviewed and analyzed to determine if indications of compromise (or other organization-defined inappropriate or unusual activities) have occurred, and the frequency of the reviews. Provide evidence from ITSD showing configuration settings that a suspicious event will send out an alert to GA-MDHE as a result of audit logs to determine if indications of compromise (or other organization-defined inappropriate or unusual activities) have occurred.

6.2.15. No Evidence provided for CONFIGURATION MANAGEMENT POLICY AND PROCEDURES (CM-1)

NIST SP 800-53 Control: CM-1	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
CM-1: CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for CONFIGURATION MANAGEMENT POLICY AND PROCEDURES (CM-1)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE CM-1.a, b)
1) Provide copies of the GA-MDHE Configuration Management Policy document.

2) Provide evidence demonstrating the GA-MDHE Configuration Management Policy has been provided to the organization-defined roles.

3) Provide evidence which confirms that the policy has been reviewed and updated by GA-MDHE with the organization-defined frequency.

SA Team Comments: No evidence provided to demonstrate documentation of a configuration management policy and procedures, and how often the policy is reviewed and updated (according to organization-defined frequency). GA-MDHE needs to document its configuration management and change management policy and process. Identify who is responsible for communicating its requirements for baseline configuration and configuration settings to ITSD. GA-MDHE needs to document what configuration settings are, and are not, allowed for its environment (e.g. allowed ports, protocols, services).

6.2.16. No Evidence provided for BASELINE CONFIGURATION (CM-2)

NIST SP 800-53 Control: CM-2	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
CM-2: BASELINE CONFIGURATION

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for BASELINE CONFIGURATION (CM-2)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE CM-2)
Provide baseline configurations which are currently used within the system (Windows, Linux, Virtual Machine (VM), Network Appliances/Devices, etc.).

SA Team Comments: No evidence provided to demonstrate baseline configurations are currently reviewed by GA-MDHE for the system (Windows, Linux, VM, Network Applications/Devices, etc.). GA-MDHE needs to document permitted, and not permitted, configuration settings for ports, protocols, and services for its environment. If GA-MDHE wants any deviance from ITSD’s baseline configurations, GA-MDHE needs to document deviances and provide to ITSD.

6.2.17. No Evidence provided for CONFIGURATION SETTINGS (CM-6)

NIST SP 800-53 Control: CM-6	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
CM-6: CONFIGURATION SETTINGS

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for CONFIGURATION SETTINGS (CM-6)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE CM-6.a, b, c, d)
Provide secure configuration guide samples and Department of Defense (DOD) System Technical Implementation Guides (STIG) used to ensure systems align with baselines.

SA Team Comments: No evidence provided to demonstrate the use of secure configuration guide samples and Internal Revenue Service (IRS) Safeguard Computer Security Evaluation Matrix (SCSEM) to ensure systems align with baselines. GA-MDHE and ITSD have accepted this finding. Nessus has been procured and both vulnerability and configuration scanning will begin on 9/20/2019. GA-MDHE must direct ITSD to perform both vulnerability and configuration scanning of GA-MDHE system boundary on a monthly basis and share scan results with both the GA-MDHE Information Security Officer (ISO) and Client Services Manager (CSM) Liaison.

6.2.18. No Evidence provided for LEAST FUNCTIONALITY (CM-7)

NIST SP 800-53 Control: CM-7	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
CM-7: LEAST FUNCTIONALITY

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for LEAST FUNCTIONALITY (CM-7)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE CM-7.a)
Provide configurations and/or policy showing that services/ports that are not needed are disabled. This can be hardening guide policies, system configuration checklists, etc.

SA Team Comments: No evidence provided to demonstrate configurations and/or policy showing services/ports that are not needed are disabled. Provide evidence for CM-2. GA-MDHE to document permitted, and not permitted, configuration settings for ports, protocols, and services for its environment. If GA-MDHE wants any deviance from ITSD’s baseline configurations, GA-MDHE needs to document deviances and provide to ITSD.

6.2.19. No Evidence provided for CONTINGENCY PLANNING POLICY AND PROCEDURES (CP-1)

NIST SP 800-53 Control: CP-1	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
CP-1: CONTINGENCY PLANNING POLICY AND PROCEDURES

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for CONTINGENCY PLANNING POLICY AND PROCUEDURES (CP-1)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE CP-1.a, b)
Provide a copy of the most recent contingency planning policy and procedures for GA-MDHE.

SA Team Comments: No evidence provided to demonstrate the most recent Contingency Planning policy and procedures for GA-MDHE. GA-MDHE shall document a Contingency Planning Policy and Procedure which includes identifying ITSD's role in the event of a disaster, and if any of the GA-MDHE information system components are not up and running. Identify the individuals from GA-MDHE who shall work with ITSD in the event of a disaster to bring the system back up and operational. Document contingency plan testing, which shall be conducted at least annually with ITSD, as well as contingency plan training.

6.2.20. No Evidence provided for CONTINGENCY PLAN TESTING (CP-4)

NIST SP 800-53 Control: CP-4	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
• CP-4: CONTINGENCY PLAN TESTING

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for CONTINGENCY PLAN TESTING (CP-4)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE CP-4.a)
Provide evidence the system undergoes contingency plan testing at least annually.

SA Team Comments: No evidence provided to demonstrate GA-MDHE participates in contingency plan testing/ Disaster Recovery (DR) exercises with ITSD for its critical components. GA-MDHE shall participate in the ITSD Contingency Plan test/ DR exercise on an annual basis. GA-MDHE is to identify which of its information system components needs to be tested (e.g. Onbase scanner, File share system storing personally identifiable information (PII)). GA-MDHE is to confirm its data stored on these devices is restored successfully from system backup.

6.2.21. No Evidence provided for MEDIA MARKING (MP-3)

NIST SP 800-53 Control: MP-3	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
MP-3: MEDIA MARKING

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for MEDIA MARKING (MP-3)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE MP-3)
1) Provide the GA-MDHE policy for media marking. Documents containing PII information should be marked as ‘Sensitive but Unclassified’.

SA Team Comments: During the onsite security assessment review, GA-MDHE stated they send out letters to borrowers and respond to letters containing PII information.

6.2.22. No Evidence provided for PROTECTION OF INFORMATION AT REST (SC-28)

NIST SP 800-53 Control: SC-28	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
SC-28: PROTECTION OF INFORMATION AT REST

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for PROTECTION OF INFORMATION AT REST (SC-28)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE SC-28)
Provide evidence which demonstrates the protection of GA-MDHE information while the information is at rest. For example, full-disk encryption.

SA Team Comments: No evidence provided to demonstrate protection of GA-MDHE information while the information is at rest.

6.2.23. No Evidence provided for SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY (SI-7)

NIST SP 800-53 Control: SI-7	**Type:** Corrective Action	**Risk: Medium**

Affected Asset(s):
SI-7: SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

Status: Additional Analysis Required

Finding Description: Evidence Request List (ERL) Review: 'No Evidence provided for SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY (SI-7)'

Threat Description: Without evidence artifacts or comments to review, the SA Team cannot comprehensively assess the security control implementation and therefore the security of the system.

Recommendation: Provide the requested documentation, technical evidence, other artifacts, or comments for the SA Team's review:

(GA-MDHE SI-7)
Provide evidence which demonstrates the capability to monitor and detect unauthorized changes to software, firmware, and information stored within the information system.

SA Team Comments: No evidence provided to demonstrate the capacity to monitor and detect unauthorized changes to software, firmware, and information stored within the information system.

Appendix A: GA-MDHE Security Onsite Review Analysis CAP

Due to FSA: Monday, September 14, 2020

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. Access Control (AC)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
AC-1	Insufficient Evidence provided for Access Control Policy and Procedures (AC-1) SA Team Comments: Evidence provided does not demonstrate policy addresses all control requirements, and dissemination of policy and procedures to organization-defined personnel or roles. The policy shall include the process for creating, enabling, modifying, disabling, and removing GA-MDHE accounts. The policy shall include the approval process for an GA-MDHE system account (e.g. background investigation, access request submitted by Office Manager, process of requesting new user account from ITSD, and assigning individuals' access permissions depending on individual's role and responsibility, security group requirements, etc.). Also include policy for conducting	(GA-MDHE AC-1.a, b) Document the GA-MDHE Access Control Policy document. Provide evidence demonstrating the GA-MDHE Access Control Policy has been provided to the organization-defined roles. Provide evidence which confirms that the procedures have been reviewed and updated by GA-MDHE with the organization-defined frequency.	Medium	Concur	DHEWD will create a comprehensive Access Control policy document that will address the AC-1, AC-2, AC-3, AC-5, AC-6 control weaknesses in addition to the rest of the AC control family.	NS	12/7/2019

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
	GA-MDHE system account monitoring and how often it is conducted. Policy should address separation of duties, least privilege, unsuccessful logon attempts, session termination, etc.						
AC-2	Insufficient Evidence provided for ACCOUNT MANAGEMENT (AC-2)	(GA-MDHE-AC-2.a, b, c, d, e, f, g, h, I, j, k) Provide evidence which documents the types of accounts used within the GA-MDHE information system (standard user, privileged user, system accounts, service accounts, shared accounts, temporary or emergency accounts), including the business function met by each type of account. Provide evidence which documents the individual or role responsible for managing each type of account used within the system.	Medium	Concur	DHEWD will create a comprehensive Access Control policy document that will address the AC-1, AC-2, AC-3, AC-5, AC-6 control weaknesses in addition to the rest of the AC control family.	NS	12/7/2019
AC-3	Insufficient Evidence provided for ACCESS ENFORCEMENT (AC-3)	Provide documentation which defines the roles and permissions associated with each role used within the system. Provide screenshots which show the effective permissions of standard user accounts, privileged user accounts, and other application accounts which are used within the system.	Medium	Concur	DHEWD will create a comprehensive Access Control policy document that will address the AC-1, AC-2, AC-3, AC-5, AC-6 control weaknesses in addition to the rest of the AC control family.	NS	12/7/2019

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
		SA Team Comments: No evidence demonstrating the effective permissions of standard user accounts, privileged user accounts, and other application accounts which are used within the system. Provide evidence documented for GA-MDHE AC-2.a. Create a roles and responsibilities matrix table listing the different types of GA-MDHE system accounts (standard user, privileged users, Onbase scanner user, System Administrator, Manager, etc.). Document the conditions for group and role membership.					
AC-4	Insufficient Evidence provided for INFORMATION FLOW ENFORCEMENT (AC-4) SA Team Comments: Evidence provided for the Palo Alto firewall was not for the GA-MDHE servers IP addresses. Provide screen shot for Palo Alto content filtering for GA-MDHE, .129 subnet.	(GA-MDHE AC-4) Provide configuration files for network devices used within the system which control the flow of information within the system (firewalls, web filtering, VPN, IDS, routers, switches, etc.). Provide screenshots of dashboards, configuration settings, access control lists, and logs which demonstrate how the system controls the flow of information traffic.	Medium	Concur	DHEWD and OA ITSD will provide evidence of firewall protection for the DHEWD servers	U	10/7/2019

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
AC-5	Insufficient Evidence provided for SEPARATION OF DUTIES (AC-5) SA Team Comments: Evidence does not demonstrate how the system separates privileges and responsibilities (ex. Roles and Responsibilities Matrix). Provide evidence documented for GA-MDHE AC-2.a. Create a roles and responsibilities matrix table listing the different types of GA-MDHE system accounts (standard user, privileged users, Onbase scanner user, System Administrator, Manager, etc.). Document the conditions for group and role membership.	(GA-MDHE AC-5.a) Provide evidence which demonstrates how the system separates privileges and responsibilities within the system (ex. Roles and Responsibilities Matrix). Provide screenshots of permissions used within the system to demonstrate the separation of duties implemented within the system.	Medium	Concur	DHEWD will create a comprehensive Access Control policy document that will address the AC-1, AC-2, AC-3, AC-5, AC-6 control weaknesses in addition to the rest of the AC control family.	NS	12/7/2019

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
AC-6	Insufficient Evidence provided for LEAST PRIVILEGE (AC-6) SA Team Comments: No evidence was provided demonstrating the Roles and Responsibilities that permissions for users and processes acting on behalf of users are only provided with permissions and access necessary to perform job function. Create a roles and responsibilities matrix table listing the different types of GA-MDHE system accounts (standard user, privileged users, Onbase scanner user, System Administrator, Manager, etc.). Document the conditions for group and role membership.	(GA-MDHE AC-6) Provide a copy of the Roles and Responsibilities Matrix (or equivalent documentation) to demonstrate that permissions for users and processes acting on behalf of users are only provided with permissions and access necessary to perform their job function.	Medium	Concur	DHEWD will create a comprehensive Access Control policy document that will address the AC-1, AC-2, AC-3, AC-5, AC-6 control weaknesses in addition to the rest of the AC control family.	NS	12/7/2019

A.2. Awareness and Training (AT)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
AT-1	No Evidence provided for SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES (AT-1) SA Team Comments: No evidence provided to demonstrate reviewing and updating of Security Awareness and Training Policy and Procedures. Security Awareness training policy should document how often the training is provided to GA-MDHE employees; if role-based security training is provided to users who have a security/sensitive role, and that security training records are documented and maintained.	(GA-MDHE AT-1.a, b) Document a GA-MDHE Security Awareness and Training Policy and procedures, then provide evidence which confirms that the policy has been reviewed and updated by GA-MDHE with the organization-defined frequency.	Medium	Concur	DHEWD will update their security awareness and training policies and procedures and review and update them on an annual basis.	NS	10/7/2019

A.3. Audit and Accountability (AU)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
AU-1	No Evidence provided for AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES (AU-1) SA Team Comments: No evidence provided to demonstrate reviewing and updating of Audit and Accountability Policy and Procedures. Document and draft an audit and accountability policy that addresses GA-MDHE auditing and logging requirements expected from ITSD; what type of events should be audited and logged; the personnel or roles allowed to select these auditable events; how often audit logs should be received from ITSD (weekly, monthly, quarterly), and how ITSD should alert GA-MDHE to certain security incidents/ suspicious activity.	(GA-MDHE AU-1.a, b) Document a GA-MDHE Audit and Accountability Policy and Procedures, then provide evidence which confirms that the policy has been reviewed and updated by GA-MDHE with the organization-defined frequency.	Medium	Concur	DHEWD will work with OA ITSD to create a new policy and procedure for reviewing auditing logs that will be provided by ITSD based on DHEWD's criteria.	NS	1/7/2020

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
AU-2	No Evidence provided for AUDIT EVENTS (AU-2) SA Team Comments: Evidence provided did not illustrate a list of auditable events and sampling of audit logs (or screenshots of audit logs) from all applicable components; servers and applications used within the system (Operating System, Database, Active Directory, Exchange, Onbase scanner, etc.). GA-MDHE needs to document and instruct ITSD on the type of events from users which will alert GA-MDHE of suspicious activity.	(GA-MDHE AU-2.a, b, c) Provide a list of the selected events to be audited within the system, 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 (Operating System, Database, Active Directory, Exchange, Onbase database, etc.).	Medium	Concur	DHEWD will work with OA ITSD to create a new policy and procedure for reviewing auditing logs that will be provided by ITSD based on DHEWD's criteria.	NS	1/7/2020
AU-3	No Evidence provided for CONTENT OF AUDIT RECORDS (AU-3) SA Team Comments: No evidence provided to demonstrate the content of audit records including: the type of event; when the event occurred; where the event occurred; the source of the event; the outcome of the	(GA-MDHE AU-3) Please see the artifacts requested for AU-2.a for details.	Medium	Concur	DHEWD will work with OA ITSD to create a new policy and procedure for reviewing auditing logs that will be provided by ITSD based on DHEWD's criteria.	NS	1/7/2020

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
	event, and the identity of any individuals or subjects associated with the event.						
AU-6	No Evidence provided for AUDIT REVIEW, ANALYSIS, AND REPORTING (AU-6) SA Team Comments: No evidence provided to demonstrate that audit records are reviewed and analyzed to determine if indications of compromise (or other organization-defined inappropriate or unusual activities) have occurred, and the frequency of the reviews. Provide evidence from ITSD showing configuration settings that a suspicious event will send out an alert to GA-MDHE as a result of audit logs to determine if indications of compromise (or other organization-defined inappropriate or unusual activities) have occurred.	(GA-MDHE AU-6.a) Provide evidence which demonstrates that audit records are reviewed and analyzed to determine if indications of compromise (or other organization-defined inappropriate or unusual activities) have occurred.	Medium	Concur	DHEWD will work with OA ITSD to create a new policy and procedure for reviewing auditing logs that will be provided by ITSD based on DHEWD's criteria.	NS	1/7/2020

A.4. Configuration Management (CM)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
CM-1	No Evidence provided for CONFIGURATION MANAGEMENT POLICY AND PROCEDURES (CM-1) SA Team Comments: No evidence provided to demonstrate documentation of a configuration management policy and procedures, and how often the policy is reviewed and updated (according to organization-defined frequency). GA-MDHE needs to document its configuration management and change management policy and process. Identify who is responsible for communicating its requirements for baseline configuration and configuration settings to ITSD. GA-MDHE needs to document what configuration settings are, and are not, allowed for its environment (e.g. allowed ports, protocols, services).	(GA-MDHE CM-1.a, b) 1) Provide copies of the GA-MDHE Configuration Management Policy document. 2) Provide evidence demonstrating the GA-MDHE Configuration Management Policy has been provided to the organization-defined roles. 3) Provide evidence which confirms that the policy has been reviewed and updated by GA-MDHE with the organization-defined frequency.	Medium	Concur	DHEWD will create a Configuration Management Policy and procedures document that outlines the baseline configuration requirements for DHEWD equipment and any deviations from OA ITSD configurations.	NS	12/7/2019

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
CM-2	No Evidence provided for BASELINE CONFIGURATION (CM-2) SA Team Comments: No evidence provided to demonstrate baseline configurations are currently reviewed by GA-MDHE for the system (Windows, Linux, VM, Network Applications/Devices, etc.). GA-MDHE needs to document permitted, and not permitted, configuration settings for ports, protocols, and services for its environment. If GA-MDHE wants any deviance from ITSD's baseline configurations, GA-MDHE needs to document deviances and provide to ITSD.	Provide baseline configurations which are currently used within the system (Windows, Linux, Virtual Machine (VM), network appliances/devices, etc.).	Medium	Concur	DHEWD will create a Configuration Management Policy and procedures document that outlines the baseline configuration requirements for DHEWD equipment and any deviations from OA ITSD configurations.	NS	12/7/2019

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
CM-6	No Evidence provided for CONFIGURATION SETTINGS (CM-6) SA Team Comments: No evidence provided to demonstrate the use of secure configuration guide samples and Internal Revenue Service - Safeguard Computer Security Evaluation Matrix to ensure systems align with baselines. GA-MDHE and ITSD have accepted this finding. Nessus has been procured and both vulnerability and configuration scanning will begin on 9/20/2019. GA-MDHE must direct ITSD to perform both vulnerability and configuration scanning of GA-MDHE system boundary on a monthly basis and share scan results with both the GA-MDHE Information Security Officer (ISO) and Client Services Manager (CSM) Liaison.	(GA-MDHE CM-6.a, b, c, d) Provide secure configuration guide samples and DOD System Technical Implementation Guides (STIG) used to ensure systems align with baselines.	Medium	Concur	OA ITSD is in the process of moving to a new scanning product that will be capable of both vulnerability and compliance scanning. DHEWD will develop new procedures to address compliance scanning once the system is in place.	U	2/7/2020

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
CM-7	No Evidence provided for LEAST FUNCTIONALITY (CM-7) SA Team Comments: No evidence provided to demonstrate configurations and/or policy showing services/ports that are not needed are disabled. Provide evidence for CM-2. GA-MDHE to document permitted, and not permitted, configuration settings for ports, protocols, and services for its environment. If GA-MDHE wants any deviance from ITSD's baseline configurations, GA-MDHE needs to document deviances and provide to ITSD.	(GA-MDHE CM-7.a) Provide configurations and/or policy showing that services/ports that are not needed are disabled. This can be hardening guide policies, system configuration checklists, etc.	Medium	Concur	DHEWD will create a Configuration Management Policy and procedures document that outlines the baseline configuration requirements for DHEWD equipment and any deviations from OA ITSD configurations.	NS	12/7/2019

A.5. Contingency Planning (CP)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
CP-1	No Evidence provided for CONTINGENCY PLANNING POLICY AND PROCUEDURES (CP-1) SA Team Comments: No evidence provided to demonstrate the most recent Contingency Planning policy and procedures for GA-MDHE. GA-MDHE shall document a Contingency Planning Policy and Procedure which includes identifying ITSD's role in the event of a disaster, and if any of the GA-MDHE information system components are not up and running. Identify the individuals from GA-MDHE who shall work with ITSD in the event of a disaster to bring the system back up and operational. Document contingency plan testing, which shall be conducted at least annually with ITSD, as well as contingency plan training.	(GA-MDHE CP-1.a, b) Provide a copy of the most recent contingency planning policy and procedures for GA-MDHE.	Medium	Concur	DHEWD will update their contingency planning policies and procedures which will include ensuring annual testing and training.	NS	1/7/2020

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
CP-4	No Evidence provided for CONTINGENCY PLAN TESTING (CP-4) SA Team Comments: No evidence provided to demonstrate GA-MDHE participates in contingency plan testing/ DR exercises with ITSD for its critical components. GA-MDHE shall participate in the ITSD contingency plan test/ DR exercise on an annual basis. GA-MDHE is to identify which of its information system components needs to be tested (e.g. Onbase scanner, File share system storing PII). GA-MDHE is to confirm its data stored on these devices is restored successfully from system backup.	(GA-MDHE CP-4.a) Provide evidence the system undergoes contingency plan testing at least annually.	Medium	Concur	The DHEWD will participate in the annual DR exercise conducted by OA ITSD. Update DHEWD procedures & begin planning with ITSD for annual DR exercise. Conduct annual DR exercise in May, 2020 and review report of results	NS	 1/7/2020 7/7/2020

A.6. Media Protection (MP)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
MP-3	No Evidence provided for MEDIA MARKING (MP-3) SA Team Comments: During the onsite security assessment review GA-MDHE stated they send out letters to borrowers and respond to letters containing PII information.	Provide the GA-MDHE policy for media marking. Documents containing PII information should be marked as 'Sensitive but Unclassified'.	Medium	Concur	DHEWD will update policies and procedures for Media Protection including marking of letters that are sent with PII information.	U	10/7/2019

A.7. Risk Assessment (RA)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
RA-5	No Evidence provided for VULNERABILITY SCANNING (RA-5) SA Team Comments: Nexpose vulnerability scans that were run in May 2019 identified 288 vulnerabilities.	(GA-MDHE RA-5.a) Remediate all vulnerabilities within defined frequencies that commensurate with the level of risk the vulnerabilities present. Provide results from, and/or reports based on, vulnerability scans which have been conducted since the last security controls assessment.	High	Concur	OA ITSD is in the process of moving to a new scanning product that will be capable of both vulnerability and compliance scanning. DHEWD will develop new procedures to address vulnerability scanning and remediation once the system is in place. Once system is in place and producing reports, DHEWD will work with ITSD to remediate vulnerabilities	U	 1/7/2020 9/7/2020

A.8. System and Communications Protection (SC)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
SC-28	No Evidence provided for PROTECTION OF INFORMATION AT REST (SC-28)	Provide evidence which demonstrates the protection of GA-MDHE information while the information is at rest. For example, full-disk encryption.	Medium	Concur	DHEWD will work with OA ITSD to ensure that DHEWD servers are protected while at rest by use of encryption or other means.	NS	3/7/2020

A.9. System and Information Integrity (SI)

FAILED CONTROL	WEAKNESS(ES)	RECOMMENDATION(S)	THREAT LEVEL	AGENCY CONCURS	CORRECTIVE ACTION(S)	STATUS	ECD
SI-2	No Evidence provided for FLAW REMEDIATION (SI-2) SA Team Comments: Although GA-MDHE is conducting monthly vulnerability scanning, there is no evidence provided to demonstrate GA-MDHE creates reports based on findings discovered during vulnerability scanning and corrects vulnerabilities.	(GA-MDHE SI-2.a, b, c, d) Provide evidence which demonstrates GA-MDHE conducts vulnerability scanning, creates reports based on findings discovered during vulnerability scanning, and corrects vulnerabilities. For example, change tickets and scan reports.	High	Concur	OA ITSD is in the process of moving to a new scanning product that will be capable of both vulnerability and compliance scanning. DHEWD will develop new procedures to address vulnerability scanning and remediation once the system is in place. Once system is in place and producing reports, DHEWD will work with ITSD to remediate vulnerabilities	U	 1/7/2020 9/7/2020
SI-7	No Evidence provided for SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY (SI-7)	Provide evidence which demonstrates the capability to monitor and detect unauthorized changes to software, firmware, and information stored within the information system.	Medium	Concur	OA ITSD will work to ensure that their policies and procedures demonstrate the capability to monitor and detect unauthorized changes to software, firmware, and information stored within DHEWD information system.	NS	1/7/2020