



FLORIDA A&M UNIVERSITY  
DIVISION OF AUDIT

**Report No. 22-23-0006**  
**Assurance Services Report**  
**DAVID MOU Audit**



**ACCOUNTABILITY • INTEGRITY • EFFICIENCY**

June 23, 2023



## FY 22-23 DAVID MOU Audit

### EXECUTIVE SUMMARY

The Division of Audit (DoA) performed an assurance review of the Department of Campus Safety and Security’s procedures related to their use of the Driver and Vehicles Information Database (DAVID) system. This review was conducted to assure compliance with the requirements of HSMV-0158-18, the active Memorandum of Understanding (MOU) that the Department of Campus Safety and Security has in place with the Department of Highway Safety and Motor Vehicles (DHSMV).

Based on our audit, we have concluded that the Department of Campus Safety and Security met the requirements of HSMV-0158-18. Adequate controls had been designed for the required control areas of the MOU, however, our review determined that certain control areas were not operating effectively, and additionally, process procedures had not been formally defined for specific areas. Our audit outcomes can be summarized in the table below:



#### User Access & Management

- The Department of Campus Safety and Security (DCSS) had not immediately inactivated users in DAVID that had separated from the Department, as required by MOU section IV.
- DCSS management stated Quarterly Quality Control Reviews were completed each quarter, however, no documentation existed to verify that the required quarterly monitoring of user activity occurred as stated.



#### Information Handling & Dissemination

- DCSS complied with Section V. Safeguarding Information of the MOU by not disclosing or disseminating DAVID information with external parties or agencies.
- DCSS had not maintained procedures outlining the reporting of DAVID misuse to DHSMV nor the process for handling DAVID misuse internally within the department.



#### User Activity Monitoring

- Testing of the user activity for a selected sample of active DAVID users concluded that no material instances that could indicate DAVID system misuse was identified for the sample of active DAVID users selected.



Legend:



Controls are in place & operating effectively



Controls are in place but not operating effectively



Controls are not in place



## TABLE OF CONTENTS

---

EXECUTIVE SUMMARY..... 2

BACKGROUND..... 4

**MOU For Law Enforcement Agency Access To DAVID** ..... 4

**DAVID MOU: FAMU DCSS** ..... 4

OBSERVATIONS & RECOMMENDATIONS..... 5

OBJECTIVES, SCOPE, & METHODOLOGY..... 8

APPENDIX A: FAMU DCSS DHSMV MOU..... 9

DISTRIBUTION..... 18

PROJECT TEAM..... 19

STATEMENT OF ACCORDANCE ..... 19



## BACKGROUND

---

### MOU For Law Enforcement Agency Access To DAVID

The DAVID system is a repository of driver and vehicle information that is collected and maintained by DHSMV as part of their statutorily mandated duties, and is accessible through the internet via a secure user name and password. The system contains records of Florida individual's driver license information such as name, address, phone number, social security number, vehicle information, medical information, and emergency contact information. Due to the confidential nature of the information contained in DAVID this information is protected against disclosure<sup>1</sup> and exempt from public records under Florida Statute<sup>2</sup>.

Access to the DAVID system may be requested by law enforcement agencies for their use in carrying out statutorily mandated law enforcement and prosecutorial functions. In these instances, an MOU is established with DHSMV to define the conditions and limitations of electronic access and use of the DAVID system by the requesting agency. Through this MOU, the requesting agency agrees to maintain the confidential and exempt status of DAVID information and agrees to abide by the information safeguarding requirements and the compliance and control measures specified by DHSMV.

### DAVID MOU: FAMU DCSS

FAMU DCSS renewed its MOU agreement with DHSMV in September 2017 with an agreement term of six years. DAVID information accessed and received by DCSS is used for University law enforcement purposes including verification of identity, traffic-related inquiries, criminal investigations, and employment background investigations. DCSS is responsible for administering and managing access and use of the DAVID system within its department, as well as protecting and maintaining information obtained from DAVID in accordance with the MOU agreement.

---

<sup>1</sup> [18 USC 2721: Prohibition on release and use of certain personal information from State motor vehicle records](#)

<sup>2</sup> [F.S. Section 119.0712\(2\): Executive branch agency-specific exemptions from inspection or copying of public records](#)



## OBSERVATIONS & RECOMMENDATIONS

Review Area	Observations	Recommendations
<b>User Access Termination</b>	<p><b><u>System Inactivation Sample</u></b></p> <ul style="list-style-type: none"> <li>MOU Section IV. <u>Statement of Work</u> subsection B-8 requires DCSS to inactivate DAVID users immediately upon separation.</li> <li>Review of the listing of separated personnel for DCSS and system-generated listing of DAVID users identified 6 active DAVID users as having separated within the last year.</li> <li>Sample testing of all 6 separated active DAVID users disclosed that all 6 separated active DAVID users were not immediately inactivated by their last date of employment.</li> </ul>	<p><b><u>Inactivation Workflow</u></b></p> <ul style="list-style-type: none"> <li>We recommend that the DCSS implement a workflow for the DAVID user inactivation process that documents the request for inactivation, the deadline (last date of employment) for inactivation, and receipt confirmation that the user was timely inactivated.</li> </ul>
<b>Quarterly Quality Control Reviews</b>	<p><b><u>Quarterly Sample</u></b></p> <ul style="list-style-type: none"> <li>MOU Section VI. <u>Compliance and Control Measures</u> requires DCSS to conduct Quarterly Quality Control Reviews (QQCR) within 10 days of the end of each quarter.</li> <li>Review of a sample of 4 completed QQCRs disclosed that each quarterly review was completed timely for each quarter.</li> <li>Review of the QQCR reports and user activity report disclosed that no documentation was maintained to exhibit that DAVID usage was monitored as part of each quarterly review.</li> </ul>	<p><b><u>Usage Monitoring Review</u></b></p> <ul style="list-style-type: none"> <li>We recommend that DCSS documents the active users that were monitored in each QQCR and implement a secondary sign-off to affirm that monitoring was conducted.</li> <li>We recommend that DCSS reviews the continued business need for access to DAVID for each of the active users as part of the QQCR process.</li> </ul>
<b>Confidentiality &amp; Unauthorized Use Training</b>	<p><b><u>User Training Review</u></b></p> <ul style="list-style-type: none"> <li>Review of annual DAVID training logs and walkthrough of the training process indicated that appropriate procedures and systems were in place to provide annual training.</li> </ul>	<p><b><u>Training Monitoring</u></b></p> <ul style="list-style-type: none"> <li>We recommend that the Department perform a verification check for active DAVID user training compliance as a part of each QQCR. We also recommend verifying that new users have completed training</li> </ul>



Review Area	Observations	Recommendations
	<ul style="list-style-type: none"> <li>A sample of 11 active DAVID users disclosed that 2 active users were not compliant with annual training.</li> </ul>	<p>prior to being given DAVID access.</p>
<p><b>Physical Access Security &amp; Retention</b></p>	<p><b><u>Compliance Review</u></b></p> <ul style="list-style-type: none"> <li>Observation of the physical access controls implemented by DCSS disclosed that appropriate controls were in place to protect office devices with access to DAVID and printed DAVID information.</li> <li>Our review of the retention of DAVID information disclosed that DAVID information was printed and retained as part of the employee background check.</li> </ul>	<p><b><u>No Recommendations</u></b></p>
<p><b>External Dissemination of DAVID Information</b></p>	<p><b><u>Compliance Review</u></b></p> <ul style="list-style-type: none"> <li>Inquiry with key personnel and review of DCSS policy disclosed that the DCSS does not disclose or share DAVID information externally nor assign duties related to the MOU to outside entities.</li> <li>Review determined that the Department complied with the information-sharing requirements of the MOU.</li> </ul>	<p><b><u>No Recommendations</u></b></p>



Review Area	Observations	Recommendations
<b>DAVID Misuse Reporting</b>	<p><b><u>Compliance Review &amp; Verification</u></b></p> <ul style="list-style-type: none"> <li>• Inquiry with key personnel disclosed appropriate procedures that DCSS follows in the case an instance of misuse is identified.</li> <li>• Inquiry with key personnel disclosed that no instances of misuse had been reported within the last 12 months.</li> <li>• Independent verification was made with DHSMV and determined that their records also indicated that no instances of misuse had been reported in the last 12 months.</li> </ul>	<p><b><u>Misuse Reporting Procedures</u></b></p> <ul style="list-style-type: none"> <li>• We recommend that DCSS formally document their DAVID misuse handling and reporting procedures internally as a standard operating procedure.</li> <li>• We recommend these procedures specify the party responsible for reporting identified misuse to DHSMV, as well as the timeframe for misuse to be reported, and disciplinary action if misuse was determined to have occurred.</li> </ul>
<b>User Activity Monitoring</b>	<p><b><u>Sample Testing</u></b></p> <ul style="list-style-type: none"> <li>• A sample of active DAVID users was selected and their activity between the period of January to December 2022 was examined against the DHSMV monitoring guidance for misuse.</li> <li>• Review of the selected sample concluded that no material instances that could indicate DAVID system misuse was identified for the sample of active DAVID users selected.</li> </ul>	<p><b><u>No Recommendations</u></b></p>



## OBJECTIVES, SCOPE, & METHODOLOGY

---

### **Objectives**

The purpose of this audit was to provide assurance that DCSS of Florida A&M University complied with the Compliance and Control Measures of HSMV-0158-18 by performing an Internal Control Attestation. This attestation will satisfy the Annual Certification required to be conducted as part of the conditions of the MOU. The assessment is designed to assess for sufficient control activities relating to the protection of DAVID information from unauthorized access, disclosure, use, or modification and that full compliance with the requirements of the MOU has been met.

### **Scope**

The scope of this audit included the controls, processes, and procedures surrounding DCSS access and use of the DAVID system and information received from it. The focus of the review was an evaluation of the control activities between the period of January 1, 2022, through January 1, 2023, outlined in HSMV-0158-18 which included:

- Quarterly Quality Control Processes
- Dissemination
- Safeguarding Information
- User Access and Permissions
- Misuse
- User Activity Monitoring

### **Methodology**

The methodology for this attestation included a review of quality control reports conducted by management, system-generated source documents for the access and activity management of in-scope user personnel, employee training materials for authorized DAVID use and guidelines, system-generated training logs, procedures and narratives for adhering to the compliance measures outlined in HSMV-0158-18, sample reports of user activity monitoring reports for a selected sample of authorized users of DAVID, and observation of the physical access and security controls employed by DCSS at their Tallahassee, Florida office premises on the Florida A&M University campus.





## APPENDIX A: FAMU DCSS DHSMV MOU



### MEMORANDUM OF UNDERSTANDING FOR LAW ENFORCEMENT AGENCY ACCESS TO DRIVER AND VEHICLE INFORMATION DATABASE SYSTEM (DAVID) Contract Number HSMV-\_\_\_\_\_

This Memorandum of Understanding (MOU) is made and entered into by and between Florida A&M Board of Trustees Division of Campus Safety, hereinafter referred to as the Requesting Party, and the Florida Department of Highway Safety and Motor Vehicles, hereinafter referred to as the Providing Agency, collectively referred to as the Parties.

#### I. Purpose

The Providing Agency is a government entity whose primary duties include issuance of motor vehicle and driver licenses, registration and titling of motor vehicles, and enforcement of all laws governing traffic, travel, and public safety upon Florida's public highways.

In carrying out its statutorily mandated duties and responsibilities, the Providing Agency collects and maintains personal information that identifies individuals. This information is stored in the Department's Driver and Vehicle Information Database system, commonly referred to as "DAVID." Based upon the nature of this information, the Providing Agency is subject to the disclosure prohibitions contained in 18 U.S.C. §2721, the Driver's Privacy Protection Act (hereinafter "DPPA"), Section 119.0712(2), Florida Statutes, and other statutory provisions.

The Requesting Party is a law enforcement agency operating under the laws and authority of the state of Florida. As a law enforcement agency, the Requesting Party may receive personal information from DAVID under the government agency exception provided in DPPA as indicated in Attachment I. The Requesting Party utilizes DAVID information for the purposes of carrying out its statutorily mandated law enforcement and prosecutorial functions.

This MOU is entered into for the purpose of establishing the conditions and limitations under which the Providing Agency agrees to provide electronic access to DAVID information to the Requesting Party. Use of the data by Requesting Party shall only be for a lawful purpose.

#### II. Definitions

For the purposes of this Agreement, the below-listed terms shall have the following meanings:

- A. DAVID – The Providing Agency's Driver and Vehicle Information Database system that accesses and transmits driver and vehicle information.
- B. Driver License Information – Driver license and identification card data collected and maintained by the Providing Agency. This information includes personal information as defined below.
- C. Emergency Contact Information (ECI) – Information contained in a motor vehicle record listing individuals to be contacted in the event of an emergency. Emergency contact information may be released to law enforcement agencies through the DAVID system for purposes of contacting those listed in the event of an emergency, as noted in Section 119.0712 (2)(c), Florida Statutes.
- D. Driver Privacy Protection Act (DPPA) – The Federal Act (see, 18 United States Code § 2721, et seq.) that prohibits release and use of personal information except as otherwise specifically permitted within the Act.
- E. Law Enforcement Agency – Any state, county or city law enforcement agency, and state attorney offices



operating under the laws and authority of the state of Florida.

- F. Insurance Record – Insurance information, such as Insurance Company name, policy type, policy status, insurance creation and expiration date provided to the Requesting Party, pursuant to Section 324.242(2), Florida Statutes.
- G. Parties - The Providing Agency and the Requesting Party.
- H. Personal Information – As described in Chapter 119, Florida Statutes, and information found in the motor vehicle record which includes, but is not limited to, the subject’s driver identification number, name, address, telephone number, social security number, medical or disability information, and emergency contact information.
- I. Point-of-Contact (POC) - A person(s) appointed by the Requesting Party as the administrator of the DAVID program in their agency.
- J. Providing Agency - The Florida Department of Highway Safety and Motor Vehicles. The Providing Agency is responsible for granting access to DAVID information to the Requesting Party.
- K. Quarterly Quality Control Review Report – Report completed each quarter by the POC to monitor compliance with this agreement. The following must be included in the Quarterly Quality Control Review Report:
  - 1. A comparison of the DAVID users by agency report with the agency user list;
  - 2. A listing of any new or inactivated users since the last quarterly quality control review; and
  - 3. Documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination.
- L. Requesting Party - Any law enforcement agency that is expressly authorized by Section 119.0712(2), Florida Statutes, and DPPA to receive personal information contained in a motor vehicle record maintained by the Providing Agency.
- M. Vehicle Information – Title and registration data collected and maintained by the Providing Agency for vehicles.

**III. Legal Authority**

The Providing Agency maintains computer databases containing information pertaining to driver’s licenses and vehicles pursuant to Chapters 317, 319, 320, 322, 328, and Section 324.242(2) Florida Statutes. The driver license and motor vehicle data contained in the Providing Agency’s databases is defined as public record pursuant to Chapter 119, Florida Statutes, and as such, is subject to public disclosure unless otherwise exempted by law.

As the custodian of the state’s driver and vehicle records, the Providing Agency is required to provide access to records permitted to be disclosed by law, and may do so by remote electronic means, pursuant to Sections 119.0712(2), 320.05, 321.23, 322.20, and 324.242(2), Florida Statutes, and applicable rules.

Under this MOU, the Requesting Party will be provided, via remote electronic means, information pertaining to driver licenses and vehicles, including personal information authorized to be released pursuant to Section 119.0712(2), Florida Statutes and DPPA. By executing this MOU, the Requesting Party agrees to maintain the confidential and exempt status of any and all information provided by the Providing Agency pursuant to this agreement and to ensure that any person or entity accessing or utilizing said information shall do so in compliance with Section 119.0712(2), Florida Statutes and DPPA. In addition, the



Requesting Party agrees that insurance policy information shall be utilized pursuant to Section 324.242(2), Florida Statutes.

This MOU is governed by the laws of the state of Florida and jurisdiction of any dispute arising from this MOU shall be in Leon County, Florida.

**IV. Statement of Work**

**A. The Providing Agency agrees to:**

1. Allow the Requesting Party to electronically access DAVID as authorized under this agreement.
2. Provide electronic access pursuant to established roles and times, which shall be uninterrupted except for periods of scheduled maintenance or due to a disruption beyond the Providing Agency's control, or in the event of breach of this MOU by the Requesting Party. Scheduled maintenance will normally occur Sunday mornings between the hours of 6:00 A.M. and 10:00 A.M.
3. Provide an agency contact person for assistance with the implementation and administration of this MOU.

**B. The Requesting Party agrees to:**

1. Utilize information obtained pursuant to this MOU, including Emergency Contact Information (ECI), only as authorized by law and for the purposes prescribed by law and as further described in this MOU. In the case of ECI, such information shall only be used for the purposes of notifying a person's registered emergency contact in the event of a serious injury, death, or other incapacitation. ECI shall not be released or utilized for any other purpose, including developing leads or for criminal investigative purposes.
2. Retain information obtained from the Providing Agency only if necessary for law enforcement purposes. If retained, information shall be safeguarded in compliance with Section V. Safeguarding Information, subsection C.
3. Ensure that its employees and agents comply with Section V. Safeguarding Information.
4. Refrain from assigning, sub-contracting, or otherwise transferring its rights, duties, or obligations under this MOU, without the prior written consent of the Providing Agency.
5. Not share, provide, or release any DAVID information to any other law enforcement, governmental agency, person, or entity not a party or otherwise subject to the terms and conditions of this MOU.
6. Protect and maintain the confidentiality and security of the data received from the Providing Agency in accordance with this MOU and applicable state and federal law.
7. Defend, hold harmless and indemnify the Providing Agency and its employees or agents from any and all claims, actions, damages, or losses which may be brought or alleged against its employees or agents for the Requesting Party's negligent, improper, or unauthorized access, use, or dissemination of information provided by the Providing Agency, to the extent allowed by law.
8. Immediately inactivate user access/permissions following termination or the determination of negligent, improper, or unauthorized use or dissemination of information. Update user access/permissions upon reassignment of users within five (5) business work days.
9. Complete and maintain Quarterly Quality Control Review Reports as defined in Section II – Definitions – J, and utilizing the form attached as Attachment II.



10. Update any changes to the name of the Requesting Party, its Agency head, its POC, address, telephone number and/or e-mail address in the DAVID system within ten calendar days of occurrence. The Requesting Party is hereby put on notice that failure to timely update this information may adversely affect the time frames for receipt of information from the Providing Agency.
11. Immediately comply with any restriction, limitation, or condition enacted by the Florida Legislature following the date of signature of this MOU, affecting any of the provisions herein stated. The Requesting Party understands and agrees that it is obligated to comply with the applicable provisions of law regarding the subject matter of this Agreement at all times that it is receiving, accessing, or utilizing DAVID information.
12. Cooperate with the Providing Agency in Field Audits conducted pursuant to Section VI. B., below.
13. Timely submit the reports and statements required in Section VI. Compliance and Control Measures, below.

**V. Safeguarding Information**

The Parties shall access, disseminate, use and maintain all information received under this Agreement in a manner that ensures its confidentiality and proper utilization in accordance with Chapter 119, Florida Statutes, and DPPA. Information obtained under this Agreement shall only be disclosed to persons to whom disclosure is authorized under Florida law and federal law.

Any person who willfully and knowingly violates any of the provisions of this section is guilty of a misdemeanor of the first degree punishable as provided in Sections 119.10 and 775.083, Florida Statutes. In addition, any person who willfully and knowingly discloses any information in violation of DPPA may be subject to criminal sanctions and civil liability.

The Parties mutually agree to the following:

- A. Information exchanged will not be used for any purposes not specifically authorized by this MOU. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, or the dissemination, sharing, copying, or passing of this information to unauthorized persons.
- B. The Requesting Party shall not indemnify and shall not be liable to the Providing Agency for any driver license or motor vehicle information lost, damaged, or destroyed as a result of the electronic exchange of data pursuant to this MOU, except as otherwise provided in Section 768.28, Florida Statutes.
- C. Any and all DAVID-related information provided to the Requesting Party as a result of this MOU, particularly data from the DAVID system, will be stored in a place physically secure from access by unauthorized persons.
- D. The Requesting Party shall comply with Rule 74-2, Florida Administrative Code, and with Providing Agency's security policies, and employ adequate security measures to protect Providing Agency's information, applications, data, resources, and services. The applicable Providing Agency security policies shall be made available to Requesting Party.
- E. When printed information from DAVID has met record retention, it shall be destroyed by cross-cut shredding or incineration in accordance with Florida law.
- F. The Requesting Party shall maintain a list of all persons authorized within the agency to access DAVID information. The list will not be provided to the Providing Agency, but shall be subject to viewing during any



field audit conducted by the Providing Agency or in the event of a violation under Section VI., D, of this MOU for the purposes of ascertaining whether the person or persons involved have been removed from the list or have otherwise had their DAVID access modified or limited.

- G. Access to DAVID-related information, particularly data from the DAVID System, will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.
- H. Under this MOU agreement, access to DAVID system shall be provided to users who are direct employees of the Requesting Party and shall not be provided to any non-employee or contractors of the Requesting Party.
- I. By signing this MOU, the Parties, through their signatories, affirm and agree to maintain the confidentiality of the information exchanged through this Agreement.

**VI. Compliance and Control Measures**

- A. **Quarterly Quality Control Review Report** – Must be completed, utilizing Attachment II, Quarterly Quality Control Review Report, within 10 days after the end of each quarter and maintained for two years.
- B. **Field Audits** – Field audits shall be conducted by the Providing Agency in order to ensure that MOU requirements concerning internal controls are being met. Field audits shall be conducted on-site by Providing Agency employees, who shall be designated as "Field Liaisons" for the purposes of this MOU. Field Liaisons shall be geographically located throughout the state. The Requesting Party shall cooperate with the Field Liaisons in conducting field audits by granting access to systems and records related to this MOU and assigning appropriate personnel to respond to information requests.

Audits shall be conducted a minimum of once, every two years. Field Liaisons shall contact the POC in order to schedule the audit. At the completion of the audit, the Field Liaison will complete a report and provide a copy to the Requesting Party within ninety (90) days of the audit date. Should the audit report conclude that deficiencies or issues exist in regard to the Requesting Party's internal controls, or access to or use of DAVID information, Providing Agency reserves the right to take, based upon the nature of the deficiencies/issues found, any or all of the following actions: audit more frequently than once, every two years; and/or suspend or terminate Requesting Party's access to DAVID information until such time as Requesting Party submits proof satisfactory to the Providing Agency that the deficiencies/issues have been corrected.

- C. **Internal Control Attestation** – This MOU is contingent upon the Requesting Party having appropriate internal controls in place at all times that data is being provided/received pursuant to this MOU to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure. The Requesting Party must submit an Attestation statement no later than 45 days after receipt of the audit report referenced in subsection B., above. The Attestation shall indicate that the internal controls over personal data have been reviewed and evaluated in light of the audit findings and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. The Attestation shall also certify that any and all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence. The Providing Agency may extend the time for submission of the Attestation upon written request by the Requesting Party. The Attestation must have an original signature of the Chief, Sheriff, or State Attorney, or person designated by Letter of Delegation to execute contracts/agreements on their behalf, may be sent via U.S. Mail, facsimile transmission, or e-mailed to the Providing Agency's Bureau of Records at the following address:

Department of Highway Safety and Motor Vehicles  
Bureau of Records  
2900 Apalachee Parkway, MS 89  
Tallahassee, Florida 32399-0500



Fax: (850) 617-5168

E-mail: [DataListingUnit@flhsmv.gov](mailto:DataListingUnit@flhsmv.gov)

- D. **Annual Certification Statement** - The Requesting Party shall submit to the Providing Agency an annual statement indicating that the Requesting Party has evaluated and certifies that it has adequate controls in place to protect the personal data from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of this MOU. The Requesting Party shall submit this statement annually, within 45 days after the anniversary date of this MOU. (NOTE: During any year in which a Field Audit is conducted, submission of the Internal Control Attestation may satisfy the requirement to submit an Annual Certification Statement.) Failure to timely submit the certification statement may result in an immediate field audit and, based upon the findings of the audit, suspension or termination of Requesting Party's access to DAVID information as indicated in subsection B., above.

In addition, prior to expiration of this MOU, if the Requesting Party intends to enter into a new MOU, a certification statement attesting that appropriate controls remained in place during the final year of the MOU and are currently in place shall be required to be submitted to the Providing Agency prior to issuance of a new MOU.

- E. **Misuse of Personal Information** – The Requesting Party must notify the Providing Agency in writing of any incident where determination is made that personal information has been compromised as a result of unauthorized access, distribution, use, modification, or disclosure, by any means, within 30 days of such determination. The statement must be provided on the Requesting Party's letterhead and include each of the following: a brief summary of the incident; the outcome of the review; the date of the occurrence(s); the number of records compromised; the name or names of personnel responsible; whether disciplinary action or termination was rendered; and whether or not the owners of the compromised records were notified. The statement shall also indicate the steps taken, or to be taken, by the Requesting Agency to ensure that misuse of DAVID data does not continue. This statement shall be mailed to the Bureau Chief of Records at the address indicated in Section VI. C., above. (NOTE: If an incident involving breach of personal information did occur and Requesting Party did not notify the owner(s) of the compromised records, the Requesting Party must indicate why notice was not provided, for example "Notice not statutorily required.")

In addition, the Requesting Party shall comply with the applicable provisions of Section 501.171, Florida Statutes, regarding data security and security breaches, and shall strictly comply with the provisions regarding notice provided therein.

**VII. Agreement Term**

This MOU shall take effect upon the date of last signature by the Parties and shall remain in effect for six (6) years from this date unless sooner terminated or cancelled in accordance with Section IX, Termination. Once executed, this MOU supersedes all previous agreements between the parties regarding the same subject matter.

**VIII. Amendments**

This MOU incorporates all negotiations, interpretations, and understandings between the Parties regarding the same subject matter, and serves as the full and final expression of their agreement. This MOU may be amended by written agreement executed by and between both Parties. Any change, alteration, deletion, or addition to the terms set forth in this MOU, including to any of its attachments, must be by written agreement executed by the Parties in the same manner as this MOU was initially executed. If there are any conflicts in the amendments to this MOU, the last-executed amendment shall prevail. All provisions not in conflict with the amendment(s) shall remain in effect and are to be performed as specified in



this MOU.

**IX. Termination**

- A. This MOU may be unilaterally terminated for cause by either party upon finding that the terms and conditions contained herein have been breached by the other party. Written notice of termination shall be provided to the breaching party; however, prior-written notice is not required and notice may be provided upon cessation of work under the agreement by the non-breaching party.
- B. In addition, this MOU is subject to unilateral termination by the Providing Agency without notice to the Requesting Party for failure of the Requesting Party to comply with any of the requirements of this MOU, or with any applicable state or federal laws, rules, or regulations, including Section 119.0712(2), Florida Statutes.
- C. This MOU may also be cancelled by either party, without penalty, upon 30 days' advanced written notice to the other party. All obligations of either party under the MOU will remain in full force and effect during the thirty (30) day notice period.

**X. Notices**

Any notices required to be provided under this MOU may be sent via U.S. Mail, facsimile transmission, or e-mail to the following individuals:

For the Providing Agency:

Chief, Bureau of Records  
2900 Apalachee Parkway  
Tallahassee, Florida 32399  
Fax: (850) 617-5168  
E-mail: [DataListingUnit@flhsmv.gov](mailto:DataListingUnit@flhsmv.gov)

For the Requesting Party:

Agency Point-of-Contact listed on the signature page.

**XI. Additional Database Access/Subsequent MOU's**

The Parties understand and acknowledge that this MOU entitles the Requesting Party to specific information included within the scope of this agreement. Should the Requesting Party wish to obtain access to other personal information not provided hereunder, the Requesting Party will be required to execute a subsequent MOU with the Providing Agency specific to the additional information requested. All MOU's granting access to personal information will contain the same clauses as are contained herein regarding audits, report submission, and the submission of Certification and Attestation statements.

The Providing Agency is mindful of the costs that would be incurred if the Requesting Party was required to undergo multiple audits and to submit separate certifications, attestations, and reports for each executed MOU. Accordingly, should the Requesting Party execute any subsequent MOU with the Providing Agency for access to personal information while the instant MOU remains in effect, the Requesting Party may submit a written request, subject to Providing Agency approval, to submit one of each of the following covering all executed MOU's: Quarterly Quality Control Review Report; Certification; and Attestation; and/or to have conducted one comprehensive audit addressing internal controls for all executed MOU's. The Providing Agency shall have the sole discretion to approve or deny such request in whole or in part or to subsequently rescind an approved request based upon the Requesting Party's compliance with this MOU and/or any negative audit findings.



**XII. Application of Public Records Law**

The Requesting Party agrees to comply with the following requirements of Florida's public records laws:

1. Keep and maintain public records required by the Department to perform the service.
2. Upon request from the Department's custodian of public records, provide the Department with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, Florida Statutes, or as otherwise provided by law.
3. Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law for the duration of the contract term and following completion of the contract if the contractor does not transfer the records to the public agency.
4. Upon completion of the contract, transfer, at no cost, to the Department all public records in possession of the Requesting Party or keep and maintain public records required by the public agency to perform the service. If the Requesting Party transfers all public records to the Department upon completion of the contract, the Requesting Party shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Requesting Party keeps and maintains public records upon completion of the contract, the contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the Department, upon request from the Department's custodian of public records, in a format that is compatible with the information technology systems of the Department.

**IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (850) 617-3101, [OGCFiling@flhsmv.gov](mailto:OGCFiling@flhsmv.gov), PUBLIC RECORDS COORDINATOR, OFFICE OF GENERAL COUNSEL, 2900 APALACHEE PARKWAY, ROOM A432, MS 02, TALLAHASSEE, FL 32399**

REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK





IN WITNESS HEREOF, the Parties hereto, have executed this Agreement by their duly authorized officials on the date(s) indicated below.

**REQUESTING PARTY:**

Florida A&M Board of Trustees Division of Campus Safety  
Agency Name  
2400 Wanish Way  
Street Address

Suite  
Tallahassee FL 37310  
City State Zip Code

BY: William Hudson, Jr.  
Signature of Authorized Official  
William Hudson, Jr.  
Printed/Typed Name  
VP Student Affairs  
Title  
9/28/2017  
Date  
William.hudsonjr@fam.u.edu  
Official Agency Email Address  
850-599-3183  
Phone Number

Agency Point-of-Contact:  
Terrence Calloway  
Printed/Typed Name  
Terrence.Calloway@fam.u.edu  
Official Agency Email Address  
850-599-3256 /  
Phone Number  
Fax Number

**PROVIDING AGENCY:**

Florida Department of Highway Safety and Motor  
Vehicles  
2900 Apalachee Parkway  
Tallahassee, Florida 32399

BY: \_\_\_\_\_  
Signature of Authorized Official  
Lisa M. Bassett  
Printed/Typed Name  
Chief, Bureau of Purchasing and Contracts  
Title  
\_\_\_\_\_  
Date

Approved as to form.  
Nail Chell 09/28/17  
FAMU Attorney Date



## DISTRIBUTION

---

### Responsible Manager

Terence Calloway, Associate Vice President of Safety/Chief of Police  
Audrey Alexander, Lieutenant

### Internal Distribution

#### **FAMU Senior Leadership Team**

Dr. Larry Robinson, Ph.D., President  
Dr. Maurice Edington, Chief Operations Officer  
Allyson Watson, Ph.D., Interim Provost and Vice President for Academic Affairs  
Linda F. Barge-Miles, Chief of Staff/Board Liaison  
Rica Calhoun, Chief Compliance and Ethics Officer  
Dr. Kyle Eidahl, Faculty Senate Representative  
Dr. Shawnta Friday-Stroud, Vice President for University Advancement  
Cynthia Henry, Executive Assistant  
Dr. William E. Hudson, Vice President for Student Affairs  
Joseph Maleszewski, Vice President for Audit  
Carmen Cummings Martin, Assistant Vice President for Alumni Affairs/University Advancement  
Robert Seniors, Vice President for Information Technology Services/Chief Information Officer  
Dr. Denise Wallace, Vice President for Legal Affairs/General Counsel  
Keith Miles, Director for Communications  
Dr. Charles A. Weatherford, Vice President for Research  
Tiffani-Dawn Sykes, Vice President and Director of Athletics  
Danielle McBeth, Director for Government Relations  
Dr. Erick Akins, Director for Title III Programs  
Rebecca Brown, Vice President for Finance and Administration/Chief Financial Officer  
Dr. Kelly McMurray, Vice President for Strategic Planning, Analysis, and Institutional Effectiveness  
Dr. Ezzeldin Aly, Faculty Senate Representative

#### **FAMU Board of Trustees**

Kelvin Lawson, Chair  
Kristin Harper, Vice Chair  
Ann Marie Cavazos, FAMU Faculty Senate President  
Craig Reed, Audit and Compliance Chair  
Otis Cliatt II  
Michael Dubose  
Natie G. Figgers  
Deveron Gibbons, J.D.  
Belvin Perry Jr.  
Kenward Stone  
Nicole Washington

### External Distribution

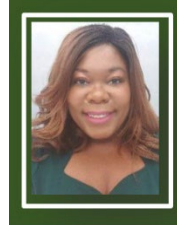
Julie Leftheris, Inspector General and Director of Compliance, Board of Governors



## PROJECT TEAM



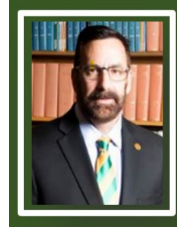
*Project Lead*  
William Thomson, CISA  
Senior IT Auditor



**Engagement was supervised by:**  
Deidre Melton, MBA, CFE, CIA,  
CISA, CISM, CDPSE, CRISC,  
CRMA, CIGI, CIG  
Associate Vice President for  
Audit and Chief Risk Officer



*Project Reviewer*  
Arriet Foster, MBA,  
CIA, CFE, CIGA,  
CIGI  
Lead Senior Auditor  
& Investigator



**Engagement was approved and distributed by:**  
Joseph K. Maleszewski, MBA,  
CIA, CISA, CGAP, CIG, CIGA,  
CIGI, CCEP, CCA, CFE  
Vice President for Audit

## STATEMENT OF ACCORDANCE

The Division of Audit’s mission is to provide independent, objective assurance and consulting services designed to add value and improve the University’s operations. It helps the University accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

We conducted this assurance service in accordance with the International Standards for the Professional Practice of Internal Auditing. Those standards require we plan and perform the assurance services to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our engagement objectives. We believe the evidence obtained provides a reasonable basis for our conclusions based on our objectives.

Please address inquiries regarding this report to the Division of Audit at (850) 412-5479.

<https://www.famu.edu/administration/audit/index.php>