

Data Protection Controls for Partner Agencies Audit Report 202021-01

August 1, 2022

Executive Summary

The Department of Highway Safety and Motor Vehicles (Department) Division of Motorist Services (MS), Bureau of Records (BOR), with assistance from Information Security Administration (ISA), are ultimately responsible for the safekeeping, guarding, and complying with laws and regulations governing the exchange of the Department's sensitive data with local, state, and federal government agencies (external agencies) who obtain motor vehicle and driver information through remote electronic means, pursuant to Section 119.0712, Florida Statutes (F.S.). Sharing Department data with an external agency poses potential risks; many of which could have adverse impacts in the form of, but not limited to; strategic, reputational, financial, legal, or information security issues. Other potential negative outcomes include service disruption and regulatory noncompliance.

The purpose of this audit was to review and evaluate the efficiency and effectiveness of data protection controls required of external agencies, not including Tax Collectors or License Plate Agencies, who access Department data and maintain compliance with applicable laws, Department policy, and procedures. Each external agency maintains a Memorandum of Understanding (MOU) data exchange agreement with the Department. We reviewed the Department's verification and selection process, data protection requirements, data recovery measures, security breach standards, contract defaults, and the levels of access by these external agencies. We also sampled MOU agreement documentation for accuracy, completeness, timeliness, and the storing of information within the Electronic Repository of Executed Contracts (EREC) system and the Data Listing Unit (DLU) Access database.

Our review determined enhancing controls for managing and storing required audit documentation and *Certification Statements* would improve oversight of external agencies. We noted there are no formal oversight procedures to verify documentation received is accurate, complete, timely, and uploaded into the EREC system and DLU Access database. The DLU unit attempts to work with the external agency when it fails to comply with the terms of the MOU before terminating its data access, yet there are no written procedures on how to handle noncompliance. BOR has recently drafted a manual for the DLU unit on requirements for inputting/updating information within the EREC system and DLU Access database, dated February 2022. We recommend the Division of MS management strengthen the verification process to ensure external agencies' compliance documentation is accurate, complete, timely, and stored in appropriate systems and databases. We also recommend the Division of MS management ensure corrective actions are taken, up to and including suspension, for

external agencies who fail to submit their compliance documentation timely. We further recommend the Division of MS management implement written procedures for exercising corrective action when external agencies fail to submit their compliance documentation timely.

Our review also determined receiving and evaluating Internal Control and Data Security (ICDS) audits for external agencies prior to providing access to Department data would strengthen security and compliance. A lack of a security assessment or an audit prior to external agencies' access to Department data impedes the Department's data protection responsibilities. We recommend the Division of MS management receive and evaluate ICDS audits prior to external agencies receiving Department data, assuring that proper data security controls are already present.

Management concurred with the findings and recommendations and has begun implementing corrective actions.

Background and Introduction

The Department is exposed to risks, as well as potential liabilities, when external agencies store, access, transmit or perform business activities for and with the Department. Managing the Department's data assets should be a high priority. Department data should be managed, secured, improved, and protected through its lifecycle. Effective contract oversight, including internal controls throughout the contract, provides a level of assurance that Department data and personal information can be protected against fraud, corruption, loss of data or data breaches.

External agencies are vetted by the Department to ensure they are eligible for access to Department data pursuant to the Federal Driver's Privacy Protection Act (DPPA) and state laws and regulations that protects driver license and motor vehicle data (Personal Identification Information). The Department requires external agencies have security requirements and standards consistent with specific Florida Statutes (F.S.), Florida Administrative Code (F.A.C.), and the Department's *External Information Security Policy*.

In accordance with Section 282.318, F.S., the Department is responsible for establishing standards and processes consistent with generally accepted best practices for information technology security, to include cybersecurity, and adopting rules that safeguard an agency's data, information, and information technology resources to ensure availability, confidentiality, and integrity and to mitigate risks. Agencies should establish asset management procedures to ensure that an agency's information technology resources are identified and managed consistent with their relative importance to the agency's business objectives.

Per Section 119.0712(2), F.S., personal information contained in a motor vehicle record is confidential and may only be released by the Department as authorized by the Federal DPPA. Emergency contact information is also considered to be protected, confidential, and exempt from disclosure unless consent of the person to whom such emergency contact information applies is given.

According to Section 501.171, F.S., "third-party agents" are entities that have been contracted to maintain, store, or process personal information on behalf of a governmental entity. Third-party agents have the duty to notify the Department of any breach of security as expeditiously as possible, but no later than 10 days following the determination of the security breach of a third-party agent.

Chapter 60GG-2, F.A.C., requires each agency ensure access to IT resources is limited to authorized users, processes, or devices, and to authorized activities and transactions. It establishes minimum requirements of controls for access to agency devices and user accounts. It also requires the use of unique user authentication for agency-owned or approved computing, periodic reviews of access rights with information owners, the removal of access rights upon separation, and the removal of unnecessary access privileges.

The Federal DPPA - describes that a Division of Motor Vehicle, and any officer, employee, or contractor, therefore, shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual obtained by the division in connection with a motor vehicle record. This act requires that personal identifiable information of the Division of Motor Vehicles' records only be disclosed under defined permissible use criteria.

The following sections describe the general processes the Department uses to manage and secure protected data that is requested and accessed by external agencies:

Selection and Verification Process

Access to Department data is a process managed mainly by the BOR's DLU unit. DLU staff operate as contract managers. MOU agreements are assigned to a DLU staff member alphabetically, based on the first letter of the requesting agency's name. The DLU staff member is responsible for assigned contracts. The Bureau of Purchasing and Contracts (BPC) operates as oversight for the contract process and the EREC system.

The Department provides data access to four types of governmental agencies: Federal, State, Local, and Law Enforcement. Data exchange MOUs are established and executed for all agencies that receive Department data through electronic means.

When a request for access to the Department data is received, the external agency is required to complete and submit five forms to the DLU section:

- *Request for Exempt Personal Information in a Motor Vehicle/Driver License Record* - to explain how the data will be used and which DPPA exemption the external agency meets;
- *Data Access Application* - attesting to any DPPA violations, breaches of data security, public website processes and data security safeguards;
- *Data Access Specifications* – to specify what data is being requested, the mode of accessing that data and applicable fee(s) per statutes;
- *Data Access Technical Specifications Questionnaire* – attest statutory eligibility to receive exempt personal information in a motor vehicle/driver license record, a description of the specific data needed and a list of the statutory and/or DPPA authority; and
- *Certification Statement* – a notarized form declaring the agency has adequate controls to protect the personal data from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of the MOU and applicable laws. This certified statement also must be deemed sufficient by a Risk Management IT Security professional. The MOU requires that an annual *Certification Statement* be received from each agency within 15 business days after the anniversary of the execution date of the MOU.

Contract managers (DLU staff) use a MOU vetting checklist form to verify that all required documents have been received, signed, and notarized (if necessary). A final approval goes through ISA and then the Department of Legal Affairs (Legal), if requesting restricted data. A MOU agreement will be initiated and routed through BPC for signatures and final approval from all parties involved. Then, all documents are uploaded into the DLU Access database and EREC by the contract manager and then they are responsible for tracking the required actions/documents. The Department only provides data to external agencies for the purposes of carrying out its statutorily mandated duties and functions.

External agencies are required to also submit an ICDS audit performed by an Inspector General or an Internal Auditor on or before the first anniversary of the MOU execution date or 120 days after the request from the Department. It must be sent via Certified U.S. Mail. The ICDS audit must evaluate the external agencies' internal controls with respect to the requirements of the MOU to ensure they are adequate to protect Department data from unauthorized access, distribution, use, modification, or disclosure. Evaluations of external agency personnel and data security policies must be included and approved by a Risk Management Information Technology (IT) Security professional. Finally, all deficiencies/issues found during the ICDS audit must be certified as corrected.

Whenever an external agency enters into a new (renewal) MOU with the Department, another ICDS audit must be performed. BOR is currently drafting a formal ICDS audit review checklist which will assist with tracking and vetting these audits for sufficiency.

Every year, following the first year's ICDS audit, the external agency must provide the Department with an annual *Certification Statement*. This is a fillable Department form that attests, under the penalty of perjury, that the external agency has read all relevant laws, policies, and manuals and confirms that the external agency's controls have been evaluated and certified as adequate to protect personal data from unauthorized access, distribution, use, modification, or disclosure, and is in full compliance with the requirements of the MOU. Failure to meet this requirement may result in an immediate termination of the MOU.

The Department also requires external agencies to implement security practices and standards consistent with Section 282.318, F.S., Chapter 60GG-2, Florida Administrative Code (F.A.C.), and the Department's *External Information Security Policy*.

Data Protection Requirements

The following controls are required of external agencies to protect Department data and are addressed in both the *External Information Security Policy* and the MOU agreement:

- Confidentiality - This addresses the Department's expectations for external agencies, which include safeguarding and maintaining the confidentiality and security of Department data in accordance with the MOU, *External Information Security Policy* and applicable state and federal laws.
- User Access - The MOU dictates that user access must be immediately removed upon a member misusing data or separating from the external agency, and user access should be updated within 5 business days when reassignment occurs. All access to the information must be monitored on an ongoing basis by the external agency. In addition, the external agency must complete an annual *Certification Statement* to ensure authorized use and the dissemination of information is in full compliance with the MOU and applicable laws and must be provided to the Department.
- Media location and device/physical security – This addresses the expectation of Department data being stored in a location that is physically and logically secure from access by unauthorized persons. *External Information Security Policy* stipulates passwords stored on physical media must be protected by encryption technology. Finally, *External Information Security Policy* dictates that workstation that houses Department data must be password protected, must have an

automatic time-out within 15 minutes of inactivity, and a maximum of 5 unsuccessful log-in attempts before the user account is locked.

- Fourth-party risk - Requirements for the external agency to impose the Department's data protection expectations to subcontractors and employees is within the MOU. For federal agencies, the external agency agrees to promptly consider and adjudicate any and all claims that may arise out of the MOU resulting from the actions of the external agency, duly authorized representatives, agents, or contractors of the external agency, and to pay for any damage or injury as may be required by federal law. All fourth-party agents or contractors are required to take the Department's training course related to Information and Cybersecurity Awareness through a PowerPoint presentation that is provided by the external agency and complete all confidential form acknowledgements. All forms are required to be kept by the external agency. Through the initial MOU vetting process, the Department confirms whether or not the Department's data is placed into any fourth-party system or server. If the external agency plans to place the data in a fourth-party server, a MOU agreement must be initiated by the Department and the fourth-party agent, who must also comply with Chapter 60GG-2, F.A.C.
- Allowable/disallowable data use - While the entire MOU serves as a reference for allowable and disallowable use, the Department may include control records in the data provided in an effort to identify misuse of the data. It also addresses protocols for Department data misuse and lists the reporting requirements for suspected and confirmed compromising of data.
- Noncompliance - This details the Department's options and potential consequences for noncompliance with any portion of the MOU and relevant laws. It further details the financial ramifications of misusing Department data via fines and/or penalties, along with Corrective Action Plans (CAP).

It is a requirement of the Department for external agencies to complete the Information Security Training on the PartnerNet portal within 30 days of receiving account access to the Department's data or risk of having access terminated. However, BOR does not ensure that the training is completed by external agencies. All external agencies must comply with the *External Information Security Policy* and MOU agreement and must submit ICDS audits and *Certification Statements* at appropriate intervals.

Data Recovery Measures

When an external agency has contracted with the Department to receive data, the external agency is accountable to notify the Department of any corruption or loss of data so that corrective action can be taken by both the Department and external agency.

The responsibility of the external agency is to report any corruption or loss of data to the Department as expeditiously as possible, but no later than 5 days of discovery. The report should include a description, time period, the number of records impacted, the harm caused, and all steps taken as of the date of the report to remedy or mitigate any injury caused and reported to BOR. The statement should also indicate the steps taken, or to be taken, by the external agency to ensure that misuse of data does not continue or recur. As soon as the Department is notified by an external agency, ISA follows all guidelines from the Department's *Information Security Policy Manual*. Failure by external agencies to meet the established requirements may result in being non-compliant and/or terminated.

In instances of noncompliance with the federal DPPA, the Department may impose liquidated damages of up to \$25 per record upon the external agency. In lieu of paying liquidated damages upon assessment, the Department may elect to temporarily suspend the MOU until paid in full. If the Department determines that the external agency is out of compliance with any of the provisions of the MOU, the Department requires the external agency to submit a CAP. The CAP should provide an opportunity for the external agency to resolve deficiencies without the Department invoking more serious remedies, up to and including MOU termination. The Department should provide the external agency with a timeframe for corrections to be made.

All external agencies must take reasonable measures to ensure that data is protected in all forms, on all media, during all phases of its life cycle, such as having unique identifiers, access control mechanisms, password protection, malware/virus protection, and ensure audit trails are maintained to protect and secure data in electronic form containing personal information. The external agency must ensure that customer records containing personal information within its custody or control are disposed of in a secure manner. As soon as the Department is notified of any corrupt or loss of data by an agency, all guidelines from the Department's *Information Security Policy Manual* will be initiated and any participants involved will be notified. An external agency must provide the Department with all information required to comply with the notification requirements, which is stipulated within the MOU agreement and the *External Information Security Policy*.

Security Breach Standards

In the event of a breach of security by an external agency, the agency must notify the Department as expeditiously as possible, but no later than 10 days following the determination of the breach or reason to believe the breach occurred with the external agency. An external agency must provide the Department with all information required to comply with the notification requirements, which is stipulated within the MOU agreement. When external agencies fail to provide proper notification, it shall be

deemed a violation of Section 501.171(6), F.S. Proper disposal of customer records is a key component for preventing breaches of security of personal information.

If ISA determines there is a data breach, ISA will follow the necessary steps provided within the Department's *Information Security Policy Manual* and report it to the appropriate levels of management and notify impacted individuals and credit reporting agencies.

Contract Defaults

The DLU unit uses an Access database and the EREC system to track and monitor compliance with the agreement between external agencies and the Department. The DLU Access database is used daily to manage data exchange MOUs, so DLU's contract managers can track or store certifications, attestation due dates, communications between the Department and external agency, received documents, reviews/audits, types of data currently being distributed to external agencies, and run queries to perform supervisory reviews. The MOU vetting checklist form is utilized for verification requirements when the MOU agreement is up for renewal and then the updated copy is uploaded to the DLU's Access database. EREC houses a multitude of details for any single contract, including term dates, vendor contact information, responsible contract manager, amendments, renewal or extension allowances, data exchange details, and the approved MOU agreement. The EREC system is the primary contract management system for the Department. All relevant contract documentation, including the MOU is found within EREC as attachments.

DLU's contract managers do not use EREC daily due to lack of database support for their processes and workflows. Contract managers have limited editing abilities within EREC and are only able to upload documents. Any changes require BPC staff assistance to modify records.

If an external agency intends to renew with the Department, prior to the expiration of the MOU, a *Certification Statement* must be submitted attesting that appropriate controls are current and to remain in place during the final year of the MOU. This should be submitted to the Department prior to issuance of a new (renewal) MOU contract.

In the event an external agency is noncompliant, it is escalated through BOR chain of command to the Chief of Records. If necessary, BOR consults with Legal and/or leadership, prior to terminating the MOU.

Access Levels

The Department determines if an external agency is eligible to receive specified or restricted data. Highly restricted personal information data that can be found in the

motor vehicle or driver record under 18 USC § 2725, includes; driver license photograph, social security number, medical and disability information. This information is not provided to private entities and is only disclosed to governmental entities such as law enforcement agencies. The Department has established File Transfer Protocol (FTP) files/processes and web services that are available if the external agency is requesting specific or qualified DPPA data. Personal information is protected, blocked, and only released via remote electronic means and approved by MS, ISA and Legal. It must go through an approval process via DocuSign. If approved, the file will be released to the external agency. FTP is used to transmit files between computers on a secure network.

The Department does not develop new processes to fit the external agency needs. Instead, the Department educates the agency on the data exchange methods available, helping to determine which process best meets their business requirement. Stipulations are required by the Department for the data levels needed.

Findings and Recommendations

Compliance Documentation

Finding No. 1: Enhancing controls for managing and storing required audit documentation and *Certification Statements* would improve oversight of external agencies.

The *National Institute of Standards and Technology's* (NIST) Risk Management Framework includes the "Assess" step which proposes that organizations should periodically ensure compliance with data protection requirements via the review and assessment of controls and their associated documentation. Further, the "Monitor" step stipulates continuous monitoring activities must be documented, especially critical authorization-related documents like assessment reports and milestone documents, such as annual statements, that support ongoing compliance.

The *ISACA Journal's* article titled, "A Risk-Based Management Approach to Third-Party Data Security, Risk, and Compliance", recommends organizations identify and mitigate the additional risks imposed by third-party agencies on an ongoing basis. Controls to address known third-party agency risks should be embedded into MOUs, should be sufficient in mitigating the risks, and must include compliance evidence requirements. Evidence of third-party agency compliance must be documented and reviewed.

We reviewed a sample of 27 data exchange MOUs to verify that each agreement had all necessary forms, audits, reviews, and were compliant with applicable laws, procedures, and received within a reasonable time. We also reviewed the EREC system and the DLU Access database.

Of the 27 data exchange MOUs we reviewed in both EREC and the DLU database:

We noted the Department did not suspend MOUs timely:

- 2 (7%) failed to provide their required security controls documentation.

We also noted missing and incomplete forms, including:

- 2 (7%) were missing the Notary Public's signature on their original *Certification Statement*;
- 1 (4%) had an annual *Certification Statement* that didn't require notarization used in place of the original, notarized *Certification Statement*; and
- 1 was missing the 2nd term year's annual *Certification Statement*.

Further, we noted the following documentation was stored in the DLU database, but not in EREC:

- 4 (15%) original, notarized *Certification Statements* were not uploaded into EREC, but 3 were found in the contract file; and
- 1 did not have its 2nd term year's annual *Certification Statement* uploaded into EREC.

There is a MOU vetting checklist and a post review checklist that is used by contract managers to ensure all compliance documentation is received, but there are no formal oversight procedures to verify documentation received is accurate, complete, and uploaded into the EREC system and DLU Access database. The DLU unit attempts to work with the external agency when it fails to comply with the terms of the MOU before terminating its data access, yet there are no written procedures on how to handle noncompliance. BOR recently drafted a manual for the DLU unit on requirements for inputting/updating information within the EREC system and DLU Access database, dated February 2022.

The absence of *Certification Statements* weakens the Department's oversight of the external agencies' compliance documentation. Additionally, incomplete or inaccurate documentation diminishes reasonable assurance that external agencies are complying with the terms of the MOU and the *External Information Security Policy*.

Recommendations

We recommend the Division of MS management strengthen the verification process to ensure external agencies' compliance documentation is accurate, complete, timely, and stored in appropriate systems and databases.

We also recommend the Division of MS management corrective actions are taken, up to and including suspension, for external agencies who fail to submit their compliance documentation timely.

We further recommend the Division of MS management implement written procedures for exercising corrective action when external agencies fail to submit their compliance documentation timely.

Management Comments

We concur. The Bureau of Records is formalizing its processes and procedures in an effort to enhance these controls and expects to complete this no later than December 31, 2022. The Bureau now only uses annual *Certification Statements* that require notarization and provides written quality assurance expectations to new Members.

ICDS Audit Process

Finding No. 2: Receiving and evaluating ICDS audits for external agencies prior to providing access to Department data would strengthen security and compliance.

The Department's data exchange MOU stipulates that the execution of the MOU is contingent upon the external agency always having appropriate internal controls in place through the duration of the MOU terms. External agencies must submit an ICDS audit from their Agency's Internal Auditor or Inspector General on or before the first anniversary of the MOU's execution date, or within 120 days from receipt of a request from the providing agency. The audit must certify that the data security procedures/policies have been approved by a Risk Management IT Security Professional and attest that all issues found during the audit have been addressed controls are in place to prevent recurrence.

NIST Special Publication 800-47 – Managing the Security of Information Exchanges dictates that, prior to activating the information exchange, implementation must include a security assessment. This security assessment should take place before the requesting agency has authorization to access data. This is to obtain assurance that the requesting agency has controls that warrant acceptable levels of risks.

We reviewed a sample of data exchange external agencies to verify that each had submitted their ICDS audit on time. We determined adequate processes exist to monitor and review these agencies' ICDS audits when required. However, there is no current process or requirement for the Department to receive and evaluate the external agencies' ICDS audit prior to gaining access to Department data.

A lack of a security assessment or an audit prior to access to Department data impedes the Department's data protection responsibilities. Similarly, absence of ongoing assessments of implemented external agencies' controls, lessens the Department's

assurance that controls are actively compliant and sufficient per the Department's data security standards.

Recommendation

We recommend the Division of MS management receive and evaluate ICDS audits prior to external agencies receiving Department data, assuring that proper data security controls are already present.

Management Response

We concur. For external government agencies requesting data access for the first time, the Department will obtain and evaluate the most recent ICDS audit prior to granting access to the data.

Purpose, Scope, and Methodology

The purpose of this audit was to review and evaluate the efficiency and effectiveness of data protection controls required of external agencies that receive Department data and maintain compliance with applicable laws, Department policy, and procedures.

The scope of this audit included data protection controls required of external agencies receiving Department data and related documentation for the 2019-2020 Fiscal Year.

The methodology included:

- Reviewing applicable statutes, rules, manuals, and procedures;
- Interviewing appropriate Department staff;
- Understanding the steps taken before entering into a contract;
- Reviewing the protection requirements to obtain data;
- Reviewing controls that prevent data from getting distributed, stolen, or maliciously released;
- Determining types and frequency of documents required for compliance;
- Selecting a sample of MOUs to verify that required forms are documented, attached within EREC and DLU Access database and are compliant and not expired, and whether the reporting and penalties for violations are defined;
- Determining if controls are in place to effectively recover Department data;
- Reviewing the Department's standards for reporting security breaches;
- Determining whether the Department has a plan that addresses steps for contract default or termination; and
- Understanding the levels in which external agencies access sensitive data.

Acknowledgement

The Office of Inspector General would like to thank ISA and MS management and BOR personnel who assisted during the audit and express our appreciation for their cooperation and valuable contributions to the Department.

Distribution, Statement of Accordance, and Project Team

Distribution

Terry L. Rhodes, Executive Director
Jennifer Langston, Chief of Staff
Boyd Dickerson-Walden, Chief Information Officer
Michelle Morris, Manager of IT Financial and Planning Services
Crill Merryday, Information Security Officer
Scott Lindsay, Chief Data Officer
Robert Kynoch, Director of Motorist Services
Richie Frederick, Deputy Director Motorist Services
Bradley Perry, Chief of Records

Melinda M. Miguel, Chief Inspector General
Sherrill F. Norman, Auditor General

Statement of Accordance

Section 20.055, Florida Statutes, requires the Florida Department of Highway Safety and Motor Vehicles' Inspector General to review, evaluate, and report on policies, plans, procedures, accounting, financial, and other operations of the Department and to recommend improvements. This audit engagement was conducted in accordance with applicable *International Standards for the Professional Practice of Internal Auditing* published by the Institute of Internal Auditors and *Principles and Standards for Offices of Inspector General* published by the Association of Inspectors General.

Project Team

Engagement conducted by:
Kim Butler, Auditor
Destiny Thomas, Auditor

Under the supervision of:
Erin Mook, Audit Director

Approved by:



Mike Stacy, Inspector General

ATTACHMENT - Management Response




Terry L. Rhodes
Executive Director

2900 Apalachee Parkway
Tallahassee, Florida 32399-0500
www.flhsmv.gov

MEMORANDUM

DATE: July 29, 2022

TO: Erin Mook, Audit Director

FROM: Robert Kynoch, Division Director 

SUBJECT: Data Protection Controls for Partner Agencies Audit (202021-01)

The following is our response to the findings and recommendations presented in the report.

Finding No.1: Enhancing controls for managing and storing required audit documentation and *Certification Statements* would improve oversight of external agencies.

Recommendations

We recommend the Division of MS management strengthen the verification process to ensure external agencies' compliance documentation is accurate, complete, timely, and stored in appropriate systems and databases.

We also recommend the Division of MS management corrective actions are taken, up to and including suspension, for external agencies who fail to submit their compliance documentation timely.

We further recommend the Division of MS management implement written procedures for exercising corrective action when external agencies fail to submit their compliance documentation timely.

Management Response

We concur. The Bureau of Records is formalizing its processes and procedures in an effort to enhance these controls, and expects to complete this no later than December 31, 2022. The Bureau now only uses Annual Certification Statements that require notarization and provides written quality assurance expectations to new Members.

Service • Integrity • Courtesy • Professionalism • Innovation • Excellence
An Equal Opportunity Employer

Our core objective is to maintain the integrity and security of Department-provided data provided to external agencies. We will document procedures no later than December 31, 2022 that consider and provide appropriate corrective actions for certain circumstances. Indeed, suspension is not always warranted, and our procedures will address other measures deemed appropriate by management.

Finding No.2: Receiving and evaluating ICDS audits for external agencies prior to providing access to Department data would strengthen security and compliance.

Recommendation

We recommend the Division of MS management receive and evaluate ICDS audits prior to external agencies receiving Department data assuring that proper data security controls are already present.

Management Response

We concur. For external government agencies requesting data access for the first time, the Department will obtain and evaluate the most recent ICDS audit prior to granting access to the data.

Cc: Mike Stacy, Inspector General