RFP: **C25019001**

Submission Deadline: June 9, 2025
4:00 pm CST

Alabama Department of Revenue

Request for Proposals

ABSTRACT

Seeking proposals from qualified professional Vendors to create and support a comprehensive Financial Institution Data Match program to import, analyze, and display data from Financial Institutions doing business in Alabama.

Alabama Department of Revenue

Collection Services Division
ATTN: Martha Pegues
375 S. Ripley Street
Montgomery, AL 36104
www.revenue.alabama.gov

Table of Contents

1.1 Definition of Terms

ALDOR - Alabama Department of Revenue

FIDM - Financial Institution Data Match

FEIN - Federal Employer Identification Number

Method I - Financial Institution sends all account files, Vendor matches files

Method II - Financial Institution sends only matched files to Vendor

RFP - Request for proposal

STAARS - State of Alabama Accounting and Resource System

SSN- Social Security Number

Vendor- Entity is bidding or has been selected to provide data matching services

STATE OF ALABAMA

REQUEST FOR PROPOSAL (RFP)
FOR
FINANCIAL INSTITUTION DATA MATCH SERVICES

Section I

1.2 Purpose

This RFP titled Request for Proposal for Financial Institution Data Match Services is issued by the Alabama Department of Revenue, hereinafter referred to as ALDOR. The overall purpose of this RFP is to seek qualified registered Vendors, hereinafter referred to as Vendor or Bidder, that have experience in the implementation of Financial Institution Data Match, hereinafter referred to as FIDM, programs for state taxing agencies. ALDOR requires a qualified company to provide FIDM services to facilitate the identification and location of delinquent taxpayer assets between ALDOR and financial institutions doing business in Alabama.

1.3 Scope and Applicability

ALDOR will have oversight approval for the life of the contract. ALDOR will make oversight decisions concerning the license and configurations of the software and service. Due to special considerations required by using a shared enterprise software agreement, ALDOR shall maintain configuration control over ALDOR's implementation of FIDM.

1.4 Background

The ALDOR Collection Services Division's, hereinafter referred to as CSD, mission is to collect past due tax amounts from final assessments issued by various tax divisions within ALDOR. When taxpayers fail to comply voluntarily, compliance is accomplished through procedures for enforcement such as issuing a Writ of Garnishment.

ALDOR has the authority to seize funds from Financial Institutions by the authority granted in The Code of Alabama (1975). The issuance of Writs of Garnishment assists ALDOR in the collection of tax dollars owed to the State. The difficult part of this process is in locating a delinquent taxpayer's bank account(s), which currently requires ALDOR to send a Writ of Garnishment to each financial institution where the taxpayer may have an account. This process is time consuming and expensive for ALDOR and has proven to be an inflated means of collecting delinquent taxes owed to the State.

FIDM is an enforcement tool that will allow ALDOR to match taxpayers who have delinquent tax liabilities with financial assets they own, which are maintained in accounts under the control of financial institutions doing business or authorized to do business in Alabama**.**

Act 2019-285 of the Alabama Legislature authorizes ALDOR to develop a FIDM program and to enter into voluntary agreements with financial institutions, or their designated data processing agents to implement a FIDM program. Pursuant to this grant of authority, ALDOR is seeking a Vendor that has proven experience in the establishment, implementation, and maintenance of direct relationships with financial institutions for the accurate matching of identified taxpayers with records of account holders at the financial institutions.

Section II

2.1 Vendor Requirement

A. The Vendor shall establish and maintain an inventory of financial institutions doing business or qualified to do business in Alabama, including trust companies, savings banks, industrial banks, commercial banks, savings and loan associations, and federal and state credit unions. The Vendor shall ensure that ALDOR is provided with the most current file listings of financial institutions doing business in or qualified to do business in Alabama.

B. The Vendor shall employ all reasonable means necessary to implement and maintain direct relationship with the financial institutions doing business in or qualified to do business in Alabama to act as the institutions' designated data processing agent for the purpose of accurately matching ALDOR identified tax delinquent records with records of account holders at the financial institutions.

C. The Vendor shall use all reasonable means necessary to facilitate the development and execution of the data match program agreement between the financial institutions and ALDOR. The agreement document shall be approved by ALDOR prior to execution by the financial institutions.

D. The Vendor shall connect financial institutions as ordered or required by ALDOR for the purpose of establishing the data connections and file requirements necessary to receive an inventory file containing matched individuals and businesses from all participating financial institutions.

E. The Vendor shall timely resolve all technical difficulties regarding the connectivity between the Vendor and the financial institutions that impact the financial institution's ability to provide the requested data using the file transfer process or participate in the data match program. The Vendor shall also resolve similar technical difficulties between the Vendor and ALDOR.

F. The Vendor shall notify ALDOR immediately upon becoming aware of a financial institution's noncompliance in providing all required data match information or services in accordance with the terms of the financial institution's agreement with ALDOR.

G. The Vendor shall under the guidance of ALDOR establish the necessary data connections with a business identified during the match process via secure file transfer program (SFTP). The connection for file transfers shall be completed within sixty (60) days after the contract is awarded, unless extended in writing by ALDOR.

2.2 Vendor Response Preparations

It is critical that a Vendor prepare comprehensive and accurate responses. Throughout this RFP the words "mandatory", "will", "shall" and "is required" are used regarding certain requirements. These requirements must be met. Failure to meet these requirements will be grounds for disqualifying a response from further consideration. Any response merely stating, "the Vendor will meet the requirements" and does not include the requested information will be disqualified from the evaluation process. The response must contain a

comprehensive description of how the Vendor meets the requirements of this RFP. A Vendor may not submit their own contract terms and conditions in response to this RFP. If they do, their response will be disqualified.

A. The State reserves the right to accept or reject any responses.

B. The Vendor, in submitting a response to this RFP, warrants that their RFP response provides all the necessary hardware, software, supplies and services to meet all the requirements and specifications of this RFP.

C. Each response must address, with a written response of compliance, each requirement in Section 2 and 3. Failure to respond to a specific requirement on these sections may be basis for a Vendor being eliminated from consideration. Each response must provide pricing for each base service. The State will not consider responses that do not provide pricing for all base services. The State will evaluate pricing based on the entire solution. Therefore, all items in the RFP will be awarded to a single Vendor.

D. At the State's Request, the Vendor will be required to furnish any information that the State may consider necessary to clarify their RFP response within three (3) business days.

E. The State is not liable for any costs or damages incurred by a Vendor in responding to this RFP.

F. RFP response must be delivered by **4:00 p.m. (CST) on June 9, 2025,** and four (4) exact copies of the RFP response must be submitted. All information is to be submitted electronically for review/approval. No questions will be answered after this date.

G. Vendor presentations may be required by ALDOR to supplement the responses. The presentation shall be at no cost to the State of Alabama.

H. Vendors are subject to minimum security criteria that must be met to be considered for use by ALDOR. As part of this selection process, the RFP applicant must demonstrate compliance with the Security Standards listed in Exhibit A by responding in writing to EVERY statement and question in the five categories. All these statements or questions may or may not be relevant to every RFP applicant. The ALDOR Information Security Section will closely review the RFP application responses and will suggest remediation measures in any area that fall short of the minimum-security criteria. ALDOR Information Security Section's approval of a given RFP applicant resides largely with the RFP applicant response to the document.

2.3 Vendor Questions

Procedural questions should be submitted by email to martha.pegues@revenue.alabama.gov and copied to Manford.jackson@revenue.alabama.gov and must be received no later than **May 27, 2025, at 4:00 p.m., (CST)**. No questions will be accepted after this date. It shall be the submitter's responsibility to ensure that ALDOR has received any questions. Confirmation can be requested via email delivery and read receipts.

Any changes or modifications to this RFP will be posted as an amendment to the RFP in STAARS (State of Alabama Accounting and Resource System).

2.4 Vendor Response Content

Answer each of the following. Please use the corresponding number, e.g., 4A, 4B, and then your response.

A. Does your company have experience in the establishment, implementation and maintenance of direct relationships with financial institutions for the purpose of Financial Institution Data Matching? If so, please describe the experience in detail.

B. Please provide a minimum of three (3) references for states in which your company is actively performing FIDM services.

C. Are you currently associated with NASPO (National Association for State Procurement Officials) or are your products and services offered on any statewide contracts that provide public cooperative purchasing/contracting? If so, please provide pertinent information.

D. Has your company ever had a contract terminated by the State for cause or has failed to complete a State contract according to the schedule or the terms within the three (3) years prior to the issuance of this RFP?

E. Please submit a cost proposal that covers a two-year period with options for renewal up to three (3) additional years. Include in your proposal any initial development fees and the fee to manage the service on a quarterly basis.

2.5 Submission of Response

Send Responses to:
Email your response to martha.pegues@revenue,alabama.gov and copy to Manford.jackson@revenue.alabama.gov.

Label your response "RFP-Financial Institution Data Match".

2.6 Submission Deadline

All responses are due at the above location no later than **4:00 p.m. (CST) on June 9, 2025**. Responses received after this date and time will not be considered. It is the Vendor's responsibility to ensure that responses are received timely and completely.

2.7 Evaluation of Proposals

Proposals will be evaluated based on the following criteria:

A. Prior experience and a record of success in providing similar services will be 75% of the total evaluation. Services considered are:
    a. Ability to reach out to and work with financial institutions (35%)
    b. Providing statistical data on the attempts (15%)
    c. Confidentiality and ability to provide validation to financial institutions (15%)
    d. Continuous updates on accounts (10%)
B. Cost/fees will be 25% of the total evaluation.

STATE OF ALABAMA

REQUEST FOR PROPOSAL (RFP)
FOR
FINANCIAL INSTITUTION DATA MATCH SERVICES

Section III

3.1 Confidentiality of Taxpayer Information

A. The Vendor shall keep all information obtained from ALDOR and the financial institutions confidential and prohibit any employee, agent or representative from disclosing that information to anyone other than the financial institutions or ALDOR.

B. The Vendor shall attest to maintaining confidentiality of information by submitting to ALDOR a signed Non-Disclosure Affidavit.

C. The Vendor shall have all employees who may encounter taxpayer information sign the Confidentiality Non-Disclosure Affidavit Acknowledgement Form certifying that they understand and shall adhere to the applicable laws regarding the confidentiality and unauthorized disclosure of tax information contained on the Non-Disclosure affidavit.

D. The Vendor shall ensure that a police criminal background check has been performed on all employees who will handle, view or access ALDOR data under this contract. This requirement also includes any new, substitute, contract or temporary employee who will handle or have access to ALDOR information. The Vendor shall provide evidence of criminal background investigations conducted for all employees who will handle, view or access ALDOR data. A background check for existing employees at the time of hire is satisfactory.

3.2 Data Matching Process

A. On a quarterly basis, ALDOR will provide the Vendor with a list of delinquent taxpayers by name and either a Social Security Number (SSN) or a Federal Employer Identification Number for match against financial institution account records. ALDOR and the Vendor shall transmit account data according to the specifications in the Multistate Financial Institutions Data Match Specifications Handbook.

B. The Vendor shall ensure that the financial institutions provide the Vendor with a depositor file, using either Method I or Method II (See 1.1 Definition of Terms) on a quarterly basis, of each account maintained at the financial institution. The depositor file shall provide the Vendor with the name and either a SSN or a FEIN of each person or business having an ownership interest in the account, together with a description of each person's interest.

C. Vendor shall transmit files to ALDOR using the same specifications.

D. This RFP is being submitted strictly for the purpose of gaining knowledge of services available on the market for the provisions of these services, related services, and options available.

E. From the information collected through this RFP, ALDOR will review all information and options related to the services, related services, and desirable options

F. All information obtained shall become the property of ALDOR upon receipt and will not be returned. ALDOR cannot guarantee that it will not be compelled to disclose all or part of any public record under the Alabama Code of Law.

G. In the RFP, ALDOR has addressed a series of questions to Vendor and requests that Vendors reply to ALDOR in the same sequence and format.

H. ALDOR also invites Vendors to submit any pertinent information that ALDOR should consider, including topics that were not included in this RFP but are relative by the same subject matter.

I. ALDOR requests that all Vendors submit responses that are short, clear, concise and complete.

J. Submitting a response to this RFP does not exclude any Vendor from submitting a response to a solicitation because of this information collected from this RFP.

3.4 Other

A. Vendors must be registered in STAARS and respond to this proposal by submitting a response to supply the manufacturer's products and services.

B. The term of this contract will be for a two-year period with options for renewal up to three (3) additional years. The contract must be signed by the Chief Procurement Officer, Contract Review Committee, and the Governor, before it is effective.

C. ALDOR shall exercise the option to renew or extend the contract under this section by giving at least ninety (90) days' notice before the initial effective term of the contract expires. The contract must be signed by the Chief Procurement Officer, Contract Review Committee, and the Governor, before it is effective.

D. Upon request, the awarded Vendor must also provide Technical Support Services during ALDOR's regular business hours at no additional charge to work directly with ALDOR staff to troubleshoot and resolve issues in a timely manner. The Vendor also must provide unrestricted access to technical information, needed for software purchased as well as access to configurations, installation, troubleshooting, and management tools. Also, the Vendor must provide software maintenance and upgrades for no additional charge. The Vendor also must submit with their bid what their basic warranty includes if the warranty exceeds the description above.

E. Disclosure – The awarded Vendor must reveal any litigation, or state or federal sanctions, they may be under that could impact the awarded Vendor's ability to fulfill their obligations under the resulting contract. Determination that a Vendor is under litigation, or state or federal sanctions, may be grounds for disqualification.

F. Force Majeure – If a Force Majeure Event is the material contributing cause of a Party's failure to perform any of its obligations hereunder, such obligations, after notifications by such Party to the other Party, shall be deemed suspended to the extent such obligations are directly affected by such Force Majeure Event, until the Force Majeure Event has ended and a reasonable period of time for overcoming the effects thereof has passed; provided, however, that if a Force Majeure Event results in the Vendor being unable to perform during any period some or all of the Services in accordance with the terms hereof, Purchasing entity shall: (i) Not be required to pay for any such Services that the Vendor is unable to

perform; (ii) Be entitled to engage an alternate Vendor, on an interim basis, to perform the Service that the Vendor is unable to perform as a result of such Force Majeure Event; (iii) Be entitled to a share of the Vendor's resources devoted to returning to full performance of Services hereunder in order to restore priority customers directly responsible for public health and safety in accordance with service level agreements for priority customers, and (iv) Have the right to terminate this contract. Both Parties shall use their best efforts to minimize delays occurring due to a Force Majeure Event. Notwithstanding the above, the Vendor shall in no event be excused from its obligations not directly affected by a Force Majeure Event (including disaster recovery services). And if the Force Majeure Event is caused by the Vendor's failure to comply with any of its obligations under this Agreement or by the Vendor's negligence or omission, there shall be no relief from any of its obligations under the Agreement.

3.5 General-Post Award

A. Invoicing Service Support - The awarded Vendor shall provide qualified financial representatives to serve as a point of contact to work with ALDOR personnel for the purpose of resolving issues and ensuring the successful invoice and payment of all software and services provided by the Vendor.

B. Change of Ownership/Assignment of Contract - In the event that there should be a material change in the awarded Vendor's corporate ownership for any reason whatsoever, ALDOR shall have the option of continuing under the contract with the awarded Vendor or its successors or assigns for the full remaining term of the contract, or immediately terminating the contract as states in the term of contract, or immediately terminating the contract as states in the State of Alabama Fiscal Procedures Manual Chapter 4-5(f). The contract will have to be amended.

C. Confidentiality Statement - The awarded Vendor shall ensure that personnel involved with any ALDOR project are advised of and acknowledge the confidential nature of information contained in ALDOR files, the safeguards required, and the criminal and civil sanctions for noncompliance in federal and state statutes. Violation of this provision is grounds for terminating the contract.

D. Post-Awards Meeting - The awarded Vendor may be required to have an orientation meeting with ALDOR. The awarded Vendor will participate at no charge to ALDOR.

The Alabama Department of Revenue appreciates your time and interest in responding to this Request for Proposal.

Alabama Department of
Revenue Information Security

Exhibit A

SECURITY STANDARDS

1.0 OVERVIEW

This document defines the minimum-security criteria that a BIDDER, any subcontractors, or partners of the BIDDER (hereinafter collectively referred to as BIDDER) must meet in order to be considered for use by the Alabama Department of Revenue (ALDOR). As part of the selection process, the BIDDER must demonstrate compliance with the Standards listed below by responding in writing to EVERY statement and question in the five categories. All of these statements or questions may or may not apply to every BIDDER. The ALDOR Information Security Section will closely review the BIDDER responses and will suggest remediation measures in any areas that fall short of the minimum-security criteria. The ALDOR Information Security Section's approval of any given BIDDER resides largely on the BIDDER's response to this document.

Criminal Code and Confidentiality Agreement – Any business entity seeking authorization to act as a BIDDER is required to comply with all state statutes and with all Department rules regarding the confidentiality of motor vehicle records, tax returns and taxpayer information, and to inform their employees concerning the provisions of the ***Code of Alabama 1975***, Section 40-2A-10; the ***Taxpayer Browsing Protection Act***, Public Law 105-35; and the ***Code of Alabama 1975***, ***Alabama Computer Crime Act***, Article 5 of Chapter 8, Title 13A. The BIDDER must adhere to the guidelines of the **National Institute of Standards and Technology (NIST) SP 800-53 (Moderate)**. Any BIDDER must also implement strict controls to ensure that ALL ALDOR data be protected at all times. Confidentiality is the concept that information is available only to authorized individuals.

This document will be revised as necessary to stay up to date with advances in security technology and to respond to changing business conditions.

2.0 SCOPE

This document can be provided to BIDDERS that are either being considered for use by ALDOR or have already been selected for use.

3.0 RESPONDING TO THESE STANDARDS

When formulating responses to questions related to compliance, the BIDDER should keep in mind that the ALDOR Information Security Section is looking for explicitly detailed, technical responses. The BIDDER must format their responses directly beneath the Standards (both questions and requirements) listed below. In addition, the BIDDER must include any security

white papers, technical documents, or policies that are appropriate.

Answers to each question should be specific and avoid generalities, e.g.:

Example:

Bad Response: "We have hardened our hosts against attack."

Good Response: All Microsoft Windows Server (list currently supported version) Software and Security updated are applied on the Saturday following "Patch Tuesday" from Microsoft at 2300 hours. Microsoft SQL Server Cumulative Update's (list currently supported SQL version and CU number) are applied after release from Microsoft on the following Saturday at 2300 hours.

4.0 STANDARDS

4.1 General Security

1. The BIDDER must ensure that no one has access to documents or confidential information for reasons other than to fulfill the BIDDER's obligation under this agreement. If the BIDDER has reason to suspect any unauthorized access or disclosure has occurred, related to ALDOR's confidential information in their possession, they must notify the ALDOR Information Security Section, by telephone within twenty-four hours and follow-up with written notification within five days.

2. The BIDDER will be required to have a background investigation done, at the BIDDER's expense, on all the BIDDER's permanent and temporary employees hired by the BIDDER involved in handling ALDOR data before the employee begins duty. The investigations must include a National level check of criminal history and assure that employees have no felony criminal convictions of any offense that involves dishonesty or breach of trust. The BIDDER must keep a copy of the investigation report in each employee's personnel folder and furnish a copy to ALDOR upon request. The BIDDER must not allow anyone access to ALDOR data that has been found to be unsuitable or unfit for assigned duties resulting from the background investigation.

3. ALDOR reserves the right to periodically audit the BIDDER's infrastructure to ensure compliance with these Standards. Network and physical audits may be conducted on site with 48 hours' notice.

4. The BIDDER must provide a proposed architecture document that includes a logical network diagram illustration, illustrating the relationship between ALDOR and any other relevant networks, with a document that details where ALDOR data resides, the applications that manipulate it, and the security thereof.

5. The BIDDER must be able to immediately disable all or part of the functionality of the system, either at the request of ALDOR or on their own initiative, should a

security issue be identified. The ALDOR Information Security Section should be notified once a security issue is identified. If after hours, the BIDDER must be able to determine the severity of the security issue and make the decision to disable the system or not.

6. The BIDDER must provide a published policy and procedure for dealing with sensitive information. This policy and procedure must include strict internal protocol that clearly defines the roles and responsibilities of service representatives and supporting staff with regard to viewing ALDOR data.

7. The BIDDER must protect stored data from unauthorized use. The BIDDER must ensure the accuracy and soundness of data at all times.

8. The BIDDER must only use test data for testing purposes, no real data will be used during the testing phase.

4.2 Physical Security

1. The equipment hosting the data for ALDOR must be in a physically secure facility which requires, at a minimum, authorized badge access. A listing of personnel with authorized badge access must be provided to ALDOR at least monthly, or as changes occur. ALDOR will have the right to inspect, at any time, the facility hosting department data.

2. ALDOR shall have final say on who is authorized to enter any locked ALDOR physical environment, as well as any restricted ALDOR logical environment.

3. ALDOR will have the right to inspect, at any time, the storage of ALDOR documents or confidential information. The BIDDER must ensure that the documents or information are stored in a secure place to prevent the compromise of any information. A representative from the BIDDER must safeguard any documents that cannot be stored in a secure place.

4. The BIDDER must disclose who amongst their personnel will have access to any data for ALDOR (both logical and physical). The BIDDER shall be held responsible for maintaining complete confidentiality on behalf of the Department. Therefore, each employee of the BIDDER permanently or temporarily assigned to this agreement, that has access to ALDOR data must sign an **"Alabama Department of Revenue Nonemployee Confidentiality and Disclosure Statement" COM: 103 (Exhibit A.1)** indicating that they understand their obligations with regard to confidentiality and disclosure of information. Civil and/or criminal penalties exist for violation of secrecy and confidentiality statutes. These "disclosure" documents must be with the employee's personnel folder kept by the BIDDER. A copy of each signed document should then be forwarded to the ALDOR Information Security Section, to the attention of the Chief Information Security Officer. The ALDOR Information

Security Section will then forward these documents to ALDOR's Human Resources Division to be kept on file.

5. Each employee of the BIDDER permanently or temporarily assigned to this agreement located on ALDOR premises must have a picture ID Badge made for identification and building access.

4.3 Network Security

1. The network hosting ALDOR's data must be logically separated from any other network or customer that the BIDDER may have. This requires that the environment hosting ALDOR resources must use logically separate network and processing hosts.

2. Data will be transferred between ALDOR and the BIDDER under the following conditions:

   The Office of Information Technology, hereinafter referred to as OIT, is ALDOR's network provider. The BIDDER will connect either via a dedicated connection, or through an Internet connection to the OIT Extranet. The type of connection, Internet or dedicated, will be agreed upon by the BIDDER and ALDOR. The management and operation of the network service and connection will follow all policies and procedures of OIT. Additional network requirements may be specified by ALDOR. **(See Exhibit A.3)**.

   If the connection is Internet, OIT will provide the appropriate firewall technology. All traffic on this connection must be protected and authenticated using cryptographic technology. **(See Cryptography below)**

4.4 Host Security

1. The BIDDER must disclose how and to what extent the hosts (Unix, Windows, etc.) comprising the ALDOR infrastructure have been hardened against attack. If the BIDDER has hardening documentation, provide that as well.

2. The BIDDER must provide a written synopsis on how and when security patches will be applied. Document should include how the BIDDER maintains awareness concerning current and emerging network security vulnerabilities, including their policy for applying security patches.

3. The BIDDER must disclose their processes for monitoring the integrity and availability of those hosts.

4. The BIDDER must comply with the following User-ID / Password requirements:

   a. Password must be 14 alpha-numeric characters and contain at least one uppercase letter, one lowercase letter, and one number or special character.

b. User-ID must be unique and must not be able to sign on to more than one location at a time.

c. Passwords are to expire every 60 days, with user being able to reset password. Application must ask user for old password, then new password, and re-verification of new password.

d. Cannot use the previous 24 passwords.

e. User access must be revoked if password is keyed wrong 3 times.

f. Auditing reports must be developed for ALDOR to audit access to the application. For example, identify who the user is, who they work for, their location, telephone number, and what access they have been granted, etc. For a full list of items to be included please contact the ALDOR Information Security Section.

5. The BIDDER must comply with the following Audit Trail requirements:

a. Create an audit trail database that can be reported from or queried, containing all user activity by function selected.

b. Data to track includes user ID, date and time the function was invoked, function (i.e., Tag Number and VIN Number).

c. Record any addition/deletion of a record and document the user ID that invoked the addition/delete function.

6. ALDOR will only allow department issued and maintained computers to be directly attached to our network. If a vendor needs access to the ALDOR network, then their computers will be attached to the DMZ of the State of Alabama Network or, if approved by ALDOR, attached to a separate domain.

4.5 Cryptography

1. The use of proprietary encryption algorithms, an algorithm that has not been made public and/or has not withstood public scrutiny (regardless of whether the developer of the algorithm is a vendor, an individual, or the government) is not allowed for any purpose.

2. Whenever possible, encryption products used should be validated by the NIST Cryptographic Module Validation Program (CMVP) and be listed on the FIPS 140-2 Cryptographic Module Validation List. These requirements aid in providing a trusted computing base for encryption services which are essential for maintaining the confidentiality of the information these systems process.

3. Encryption methods that utilize either the Triple Data Encryption Standard (Triple DES) or the Advanced Encryption Standard (AES) are acceptable. Encryption methods shown below can also be used to protect sensitive and confidential information:

- Virtual Private Network (VPN) – allows information to be sent securely between two end stations or networks over an un-trusted communications medium; use of VPN technology is the preferred method for securing sensitive and confidential communications.
- IP Security (IPSEC) – is suitable for all types of Internet Protocol (IP) traffic and may be used to secure Internet and other IP communications within State and agency networks and to connect to authorized external customers.
- TLS 1.2 and 1.3 – may be deployed to provide secured access to sensitive and confidential information on Web servers.
- Secure Shell (SSH) – may be utilized for the remote administration of sensitive systems.

Other methods of encryption require explicit approval of ALDOR before being used to protect State data or systems.

4. Symmetric cryptosystems (such as AES) require a minimum 256-bit key length. Asymmetric cryptosystems (such as RSA) require key lengths equivalent to a 256-bit or longer symmetric key. Example: A 3072-bit RSA key is equivalent to a 256-bit symmetric key.

5. Connections to the BIDDER utilizing the Internet must also be protected using a firewall with appropriate security measures, such as validation rules, Intrusion Detection Systems, Packet Sniffers, etc.