Attachment F

Contract Draft

*Required Contract Terms and Conditions by Office of Personal Service and Contract Review Rule and Regulation are *Italicized*

STATE OF MISSISSIPPI
MISSISSIPPI DEPARTMENT OF EMPLOYMENT SECURITY
CONTRACT FOR PRINTING AND MAILING SERVICES

This Professional Services Agreement (hereinafter referred to as "Contract" or "Agreement") is entered into by and between _____(hereinafter referred to as "Contractor"), having its principal place of business at _____ and the Mississippi Department of Employment Security (hereinafter referred to as "MDES" or "State"), having its principal place of business at 1235 Echelon Parkway, Jackson, MS 39213.

Article 1 - Purpose

Contractor will provide Printing and Mailing Services to support the agency. These services include printing, sorting, folding, inserting, and mailing along with return mail processing services. Contractor shall meet rigorous quality standards and specific timelines standards along with developing new processes to create more efficient and effective methods to meet the agency's printing and postal needs.

Article 2 - Term of Agreement

This Professional Services Agreement shall be from September 27, 2026, until September 26, 2029 MDES reserves the right to renew the contract for up to one term for (2) additional years at the sole discretion of the Agency. The renewal of the contract is contingent upon the receipt of funds, satisfactory performance by the Contractor during initial term, and approval by the Public Procurement Review Board. Any renewal will be at the same terms and condition as the initial term.

Article 3 – Scope of Services

The Contractor will perform, in a manner deemed by MDES to be timely and satisfactory, the services described in RFP 2026-01 Section 4 captioned as "Scope of Work," attached hereto as Exhibit "A," and the Contractor's submitted response to RFP 2026-01 captioned as "Scope of Work – Detailed Responses" attached hereto as Exhibit "B" and hereby made part of this Agreement.

Article 4 - Consideration and Method of Payment

The total compensation to be paid to Contractor by MDES under this Agreement for services performed shall not exceed the sum of _____ payable monthly at a rate of _____.

MDES has the right to deny all or any portion of cash payment to the Contractor, based upon any of the following:

- Failure to comply with any Agreement provision, all of which are deemed to be material;
- Failure to comply with applicable laws, rules, policies, or procedures;
- Failure to resolve costs disallowed under this or any separate MDES Agreement; and

- Failure to repay amounts otherwise owed to MDES.

Article 5 - Applicable Law

The contract shall be governed by and construed in accordance with the laws of the State of Mississippi, excluding its conflicts of laws provisions, and any litigation with respect thereto shall be brought in the courts of Mississippi.

Article 6 - Availability of Funds

It is expressly understood and agreed that the obligation of Agency to proceed under this agreement is conditioned upon the appropriation of funds by the Mississippi State Legislature and the receipt the appropriated funds. If the funds anticipated for the continuing time fulfillment of the agreement are, at any time, not forthcoming or insufficient, regardless of the source of funding, Agency shall have the right upon 10 business days written notice to Contractor, to terminate this agreement without damage, penalty, cost or expense to the Agency of any kind whatsoever. The effective date of termination shall be as specified in the notice of termination.

Article 7 - Compliance with Equal Opportunity in Employment Policy

Contractor understands that the Agency is an equal opportunity employer and therefore, maintains a policy which prohibits unlawful discrimination based on race, color, creed, sex, age, national origin, physical handicap, disability, genetic information, or any other consideration made unlawful by federal, state, or local laws. All such discrimination is unlawful, and Contractor agrees during the term of the agreement that Contractor will strictly adhere to this policy in its employment practices and provision of services.

Article 8 – Americans with Disabilities Act (ADA) Compliance

The Contractor shall comply with the Americans with Disabilities Act of 1990 (ADA), as amended, and the regulations issued under 28 C.F.R. Part 35, Title II, which prohibit discrimination on the basis of disability by public entities. The Contractor agrees to perform all services under this Agreement in a manner that enables MDES to meet its ADA obligations, including providing accessible communications, systems, facilities, and services. Any public-facing or MDES-facing portals, documents, or communications produced under this Agreement shall be accessible to individuals with disabilities in accordance with applicable federal and state accessibility standards. Failure to comply with this provision shall be considered a material breach of this Agreement.

Article 9 - Compliance with Laws

Contractor shall comply with, and all activities under this agreement shall be subject to, all applicable federal, state, and local laws and regulations, as now existing and as may be amended or modified.

Article 10 – Drug-Free Workplace Act Compliance

The Contractor shall comply with the Drug-Free Workplace Act of 1988 (41 U.S.C. § 8102) and all applicable regulations, including 48 C.F.R. Subpart 23.5. The Contractor shall maintain a drug-free workplace and shall implement all required measures, including publishing a drug-free workplace statement, providing a drug-free awareness program, notifying employees of obligations regarding workplace drug violations, reporting employee convictions to the appropriate authorities, and taking

required personnel actions following any such conviction. The Contractor shall make a good-faith effort to maintain compliance throughout the performance of this Agreement. Failure to comply with this Article shall constitute a material breach of the Agreement and may result in suspension of payments, termination for default, or other remedies available to the State.

Article 11 - E-Payment

Contractor agrees to accept all payments in United States currency via the State of Mississippi's electronic payment and remittance vehicle. The Agency agrees to make payment in accordance with Mississippi "Timely Payments for Purchases by Public Bodies" laws, which generally provide for payment of undisputed amounts by the Agency within 45 calendar days of receipt of invoice. Mississippi Code Annotated § 31-7-301, et seq.

Article 12 - E-Verification

If applicable, Contractor represents and warrants that it will ensure its compliance with the Mississippi Employment Protection Act and will register and participate in the status verification system for all newly hired employees. Mississippi Code Annotated §§ 71-11-1 and 71-11-3. Contractor agrees to provide a copy of each verification upon request of the [Agency] subject to approval by any agencies of the United States Government. Contractor further represents and warrants that any person assigned to perform services hereafter meets the employment eligibility requirements of all immigration laws.

The breach of this clause may subject Contractor to the following:

(1) termination of this contract and exclusion pursuant to Chapter 15 of the Public Procurement Review Board Office of Personal Service Contract Review Rules and Regulations; (2) the loss of any license, permit, certification or other document granted to Contractor by an agency, department, or governmental entity for the right to do business in Mississippi; or (3) both.

In the event of such termination, Contractor would also be liable for any additional costs incurred by the Agency due to Contract cancellation or loss of license or permit to do business in the state.

Article 13 - Paymode

Payments by Agency using the state's accounting system shall be made and remittance information provided electronically as directed by the state and deposited into the bank account of Contractor's choice. The Agency may, at its sole discretion, require Contractor to electronically submit invoices and supporting documentation at any time during the term of this Agreement. Contractor understands and agrees that the Agency is exempt from the payment of Mississippi taxes. All payments shall be in United States currency.

Article 14 - Procurement Regulations

This contract shall be governed by the applicable provisions of the Public Procurement Review Board Office of Personal Service Contract Review Rules and Regulations, a copy of which is available on the Mississippi Department of Finance and Administration's website (www.dfa.ms.gov). Any offeror responding to a solicitation for personal and professional services and any contractor doing business with a state Agency is deemed to be on notice of all requirements therein.

Article 15 – Procurement of Recovered Materials (45 C.F.R. §75.331)
Contractor agrees to comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. In accordance with 45 C.F.R. §75.331 and 40 C.F.R. Part 247, Contractor shall procure, to the maximum extent practicable, products containing the highest percentage of recovered materials when:

(1) the purchase price of the item exceeds ten thousand dollars ($10,000), or
(2) the total value of such items procured by Contractor during the preceding fiscal year exceeded ten thousand dollars ($10,000).

Contractor shall comply with all applicable standards and guidelines issued by the Environmental Protection Agency (EPA) for designated items, including but not limited to paper and paperboard products, non-paper office products, and other items identified in 40 C.F.R. Part 247. Contractor shall also procure solid waste management services in a manner that maximizes energy and resource recovery and shall establish and maintain an affirmative procurement program for recovered materials as required by federal law.
Compliance with these requirements is a material condition of this Agreement.

Article 16 - Property Rights

Property rights do not inure to Contractor until such time as services have been provided under a legally executed contract. Contractor has no legitimate claim of entitlement to the provision of work hereunder and acknowledges that the Agency may terminate this contract at any time for its own convenience.

Article 17 - Representation Regarding Contingent Fees

Contractor represents that it has not retained a person to solicit or secure a state contract upon an agreement or understanding for a commission, percentage, brokerage, or contingent fee, except as disclosed in Contractor's bid or proposal.

Article 18 - Representation Regarding Gratuities

Contractor represents that it has not, is not, and will not offer, give, or agree to give any employee or former employee of Agency a gratuity or offer of employment in connection with any approval, disapproval, recommendation, development, or any other action or decision related to the solicitation and resulting contract. Contractor further represents that no employee or former employee of Agency has or is soliciting, demanding, accepting, or agreeing to accept a gratuity or offer of employment for the reasons previously stated; any such action by an employee or former employee in the future, if any, will be rejected by contractor. Contractor further represents that it is in compliance with the Mississippi Ethics in Government laws, codified at Mississippi Code Annotated §§ 25-4-101 through 25-4-121, and has not solicited any employee or former employee to act in violation of said law.

Article 19 – Conflict of Interest Compliance

The Contractor shall comply with all federal conflict of interest requirements applicable to federally funded contracts, including 45 C.F.R. § 75.112(a)–(b), 45 C.F.R. § 75.327, and 45 C.F.R. § 75.328.

The Contractor shall avoid any organizational or personal conflicts of interest that could impair its objectivity or independence in performing under this Agreement. The Contractor shall disclose in writing to MDES any potential or actual conflict of interest as soon as it becomes known. Failure to disclose a conflict of interest or to comply with this Article shall constitute a material breach of this Agreement.

Article 20 - Required Public Records And Transparency

Upon execution of a contract, the provisions of the contract which contain the personal or professional services provided, the unit prices, the overall price to be paid, and the term of the contract shall not be deemed to be a trade secret or confidential commercial or financial information pursuant to Mississippi Code Annotated § 25-61-9(7). The contract shall be posted publicly on www.transparency.ms.gov and shall be available for at the Agency for examination, inspection, or reproduction by the public. The contractor acknowledges and agrees that the Agency and this contract are subject to the Mississippi Public Records Act of 1983 codified at Mississippi Code Annotated §§ 25-61-1, et seq. and its exceptions, Mississippi Code Annotated § 79-23-1, and the Mississippi Accountability and Transparency Act of 2008, codified at Mississippi Code Annotated §§ 27-104-151, et seq.

Article 21 - Stop Work Order

The Agency may, by written order to Contractor at any time, require Contractor to stop all or any part of the work called for by this contract. This order shall be for a period of time specified by the Agency. Upon receipt of such an order, Contractor shall forthwith comply with its terms and take all reasonable steps to minimize any further cost to the Agency. Upon expiration of the stop work order, Contractor shall resume providing the services which were subject to the stop work order, unless the Agency has terminated that part of the agreement or terminated the agreement in its entirety. The Agency is not liable for payment for services which were not rendered due to the stop work order.

Article 22 - Termination

Termination for Convenience. The Agency may, when the interests of the Agency so require, terminate this contract in whole or in part, for the convenience of the Agency. The Agency shall give written notice of the termination to Contractor specifying the part of the contract terminated and when termination becomes effective. Contractor shall incur no further obligations in connection with the terminated work and on the date set in the notice of termination Contractor will stop work to the extent specified. Contractor shall complete the work not terminated by the notice of termination and may incur obligations as are necessary to do so.

Termination for Default. If the Agency gives the Contractor a notice that the personal or professional services are being provided in a manner that is deficient, the Contractor shall have 30 days to cure the deficiency. If the Contractor fails to cure the deficiency, the Agency may terminate the contract for default and the Contractor will be liable for the additional cost to the Agency to procure the personal and professional services from another source. Termination under this paragraph could result in Contractor being excluded from future contract awards pursuant to Chapter 15 of the Public Procurement Review Board Office of Personal Service Contract Review Rules and Regulations. Any termination wrongly labelled termination for default shall be deemed a termination for convenience.

Article 23 - Termination Upon Bankruptcy

This contract may be terminated in whole or in part by Agency upon written notice to Contractor, if Contractor should become the subject of bankruptcy or receivership proceedings, whether voluntary or involuntary, or upon the execution by Contractor of an assignment for the benefit of its creditors. In the event of such termination, Contractor shall be entitled to recover just and equitable compensation for satisfactory work performed under this contract, but in no case shall said compensation exceed the total contract price.

Article 24 - Trade Secrets, Commercial and Financial Information

It is expressly understood that Mississippi law requires that the provisions of this contract which contain the commodities purchased or the personal or professional services provided, the price to be paid, and the term of the contract shall not be deemed to be a trade secret or confidential commercial or financial information and shall be available for examination, copying, or reproduction.

Article 25 - Anti-assignment/Subcontracting

Contractor acknowledges that it was selected by the State to perform the services required hereunder based, in part, upon Contractor's special skills and expertise. Contractor shall not assign, subcontract, or otherwise transfer this agreement, in whole or in part, without the prior written consent of the State, which the State may, in its sole discretion, approve or deny without reason. Any attempted assignment or transfer of its obligations without such consent shall be null and void. No such approval by the State of any subcontract shall be deemed in any way to provide for the incurrence of any obligation of the State in addition to the total fixed price agreed upon in this agreement. Subcontracts shall be subject to the terms and conditions of this agreement and to any conditions of approval that the State may deem necessary. Subject to the foregoing, this agreement shall be binding upon the respective successors and assigns of the parties.

Article 26 - Approval

It is understood that if this contract requires approval by the Public Procurement Review Board and/or the Mississippi Department of Finance and Administration Office of Personal Service Contract Review and this contract is not approved by the PPRB and/or OPSCR, it is void and no payment shall be made hereunder.

Article 27 - Attorney's Fees and Expenses

Subject to other terms and conditions of this agreement, in the event Contractor defaults in any obligations under this agreement, Contractor shall pay to the State all costs and expenses (including, without limitation, investigative fees, court costs, and attorney's fees) incurred by the State in enforcing this agreement or otherwise reasonably related thereto. Contractor agrees that under no circumstances shall the customer be obligated to pay any attorney's fees or costs of legal action to Contractor.

Article 28 - Authority to Contract

Contractor warrants: (a) that it is a validly organized business with valid authority to enter into this agreement; (b) that it is qualified to do business and in good standing in the State of Mississippi; (c) that entry into and performance under this agreement is not restricted or prohibited by any loan, security, financing, contractual, or other agreement of any kind; and, (d) notwithstanding any other provision of this agreement to the contrary, that there are no existing legal proceedings or prospective

legal proceedings, either voluntary or otherwise, which may adversely affect its ability to perform its obligations under this agreement.

Article 29 - Information Designated by Contractor as Confidential

Any disclosure of those materials, documents, data, and other information which Contractor has designated in writing as proprietary and confidential shall be subject to the provisions of Mississippi Code Annotated §§ 25-61-9 and 79-23-1. As provided in the contract, the personal or professional services to be provided, the price to be paid, and the term of the contract shall not be deemed to be a trade secret, or confidential commercial or financial information.

Any liability resulting from the wrongful disclosure of confidential information on the part of Contractor or its subcontractor shall rest with Contractor. Disclosure of any confidential information by Contractor or its subcontractor without the express written approval of the Agency shall result in the immediate termination of this agreement.

Article 30 – Data Security, Confidentiality, IRS Publication 1075 Compliance, and Federal/State Requirements

The Contractor acknowledges that, in the performance of this Agreement, it may receive, process, print, store, transmit, or otherwise have access to confidential information belonging to MDES, including but not limited to Unemployment Insurance ("UI") information, Personally Identifiable Information ("PII"), financial information, and Federal Tax Information ("FTI"). Contractor agrees to safeguard all such information in strict compliance with federal and state law, including the Privacy Act of 1974, the Social Security Act (including 42 U.S.C. §303 and Titles III, IX, and XIII), 20 CFR 603, 2 C.F.R. Part 2900, OMB Circular A-108, Mississippi Employment Security Law, applicable Mississippi statutes and regulations, MDES policies, and Internal Revenue Service ("IRS") Publication 1075.

The Contractor shall establish, implement, maintain, and enforce throughout the term of this Agreement a comprehensive data and network security program providing all administrative, technical, environmental, and physical safeguards necessary to protect MDES systems, infrastructure, and data against unauthorized access, disclosure, modification, use, processing, destruction, or loss. At a minimum, Contractor's obligations shall include the following:

(1) **Compliance With IRS Publication 1075**
Contractor shall comply with all requirements of IRS Publication 1075, including all exhibits and mandatory safeguard requirements applicable to the receipt, storage, processing, transmission, use, and destruction of FTI. IRS Publication 1075, including Exhibit 7 (Safeguard Requirements for Contractors), as may be amended or revised during the term of this Agreement, is incorporated herein by reference with the same force and effect as if fully stated herein. Contractor shall implement all administrative, physical, and technical controls required therein.

(2) **Use and Disclosure Restrictions**
Contractor shall use MDES data only for the specific purposes authorized under this Agreement and shall not re-disclose such data except as required by law or expressly authorized in writing by MDES. Contractor shall ensure that all data is accessible only to personnel who require such access in the official performance of their duties.

(3) **Personnel Requirements**

Contractor shall ensure that all personnel with access to MDES data, including FTI, complete all federally required confidentiality and security training. For personnel with access to FTI, Contractor shall comply with all IRS Publication 1075 background investigation requirements, including all applicable criminal history, identity verification, and suitability standards. Contractor shall obtain and maintain signed confidentiality agreements for all personnel with access to MDES data and shall provide such agreements to MDES upon request.

(4) **Physical and System Security**

Contractor shall secure all systems, networks, facilities, transmission channels, portable media, and storage environments containing MDES data in accordance with federal, state, and industry standards and all requirements of IRS Publication 1075. Contractor shall ensure that data is encrypted during receipt, transmission, storage, maintenance, use, and disposal.

(5) **Audit and Inspection Rights**

Contractor shall maintain systems and processes sufficient to allow an audit of compliance with this Article. MDES, the IRS, the U.S. Department of Labor, and other authorized government officials shall have the right to perform inspections, audits, reviews, and safeguard assessments of Contractor's facilities, systems, and policies, including any subcontractor, to ensure compliance with applicable requirements. Contractor shall provide full cooperation, access, documentation, and personnel as required.

(6) **Subcontractors**

Contractor shall not disclose MDES data to any subcontractor without the express written approval of MDES. Any approved subcontractor shall be bound by all requirements of this Article and IRS Publication 1075. Contractor shall remain responsible for subcontractor compliance.

(7) **Data Transmission, Storage, and Retention**

Contractor shall transmit data only through secure, MDES-approved methods. Data shall be stored only in physically and electronically secure environments. Contractor shall not archive MDES data or FTI and shall not retain such data longer than necessary to fulfill the purpose of this Agreement. Contractor shall comply with all federal and state data-retention requirements.

(8) **Breach Notification**

Contractor shall notify MDES immediately upon discovering any actual or suspected breach, loss, compromise, unauthorized disclosure, or misuse of MDES data or systems. For incidents involving FTI, Contractor shall comply with all IRS Publication 1075 incident-reporting requirements. Contractor shall provide written documentation of the incident, proposed corrective actions, and timelines for mitigation, and shall cooperate fully with MDES and the IRS in all investigative and remedial efforts.

(9) **Destruction of Data**

Contractor shall destroy all MDES data, including PII and FTI, using secure destruction methods compliant with IRS Publication 1075 and MDES requirements. Paper records shall be destroyed using cross-cut shredders producing particles 1 mm × 5 mm or smaller, or by equivalent disintegration methods. Electronic media shall be destroyed using industry-accepted secure media destruction processes. Destruction must be witnessed by a second individual, and Contractor shall provide MDES with written certification of destruction within thirty (30) days of data disposal or contract termination.

(10) **Other Security Obligations**

Contractor shall take all additional measures reasonably necessary to maintain the security and confidentiality of MDES data and to comply with MDES information-security policies, federal and state law, including but not limited to 20 CFR 603.9 and IRS Publication 1075. Contractor must immediately notify MDES of any system, hardware, or software changes affecting the processing or security of MDES data.

This Article shall survive the termination or completion of this Agreement and shall be binding upon Contractor, its employees, agents, successors, assigns, subcontractors, and any other parties acting on Contractor's behalf.

Article 31 - Data Breach Notification

To the extent applicable, Contractor represents and warrants that it will comply with the state's data breach notification laws codified at Section 75-24-29 of the Mississippi Code Annotated (Supp. 2012). Further, to the extent applicable, Contractor represents and warrants that it will comply with the applicable provisions of the HIPAA Privacy Rule and Security Regulations (45 CFR Parts 160, 162 and 164) ("Privacy Rule" and "Security Regulations", individually; or "Privacy and Security Regulations", collectively); and the provisions of the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (the "HITECH Act").

Article 32 - Compliance with MDES Artificial Intelligence (AI) Use And Governance Policy

(1) If applicable, Contractor and MDES understand and agree that all products and services provided by the Contractor under this Contract must allow the State to be and remain in compliance with the Mississippi Department of Employment Security's Artificial Intelligence Use and Governance Policy, provided as Exhibit B and C, as may be amended.
(2) MDES shall have intellectual property rights and/or licenses to the output from any work under this Contract.
(3) Contractor shall provide to the State a non-infringement warranty for claims by the Contractor and third parties for improper use of AI content. Further, Contractor acknowledges that when it uses any Large Language Models (LLMs) as part of the products and/or services provided under this Contract, it has performed infringement searches on the same and certifies that any LLMs to be used have the necessary third-party consent and licenses as applicable.
(4) Contractor agrees that with respect to uptime/predictive power of the AI tool, it shall comply with the percentages specified in the MDES AI Use and Governance policy for accuracy, precision, consistency of answers, and speed of response time to customer questions.
(5) Contractor agrees that it shall conduct response verification and/or supplement the customized AI tool using a separate accuracy-checking solution at least once every two (2) months while the tool is in use by MDES.
(6) Contractor shall comply with the State of Mississippi laws and regulations addressing AI whenever enacted and amended by the State. If the AI laws, regulations, or executive orders of the State limit the use of AI as already implemented or planned to be implemented by the State, the Contractor agrees to negotiate with the State to revise any work under this Contract to conform with said laws, regulations, or executive orders of the State.
(7) Contractor agrees to mitigate the risks presented by the use of AI to the MDES and its data in accordance with the AI governance policy of the State as appropriate.

As applicable, Contractor shall:

(8) Supply and update all technical documentation related to the AI tool as customized for the State.
(9) Maintain and update the logging capabilities of the AI tool as customized for the State.
(10) Provide documentation and training as necessary for the State to conduct proper oversight of the services and Work Products that incorporate an AI tool.
(11) Provide and maintain industry-standard cybersecurity tools to safeguard the AI tool and secure the gateways to State data incorporated in any services and the Work Products owned by or developed for the State that interface with or incorporate the AI tool.

The Contractor agrees to notify the State within the time specified of any anomalous results or failure of a customized product that incorporates artificial intelligence to minimize the adverse effects on the customers of the State, registered employers and unemployment insurance claimants. The State reserves the right to modify this notification deadline and requirement in the event that an executive order, state and federal law or regulation requires a different interval or the business needs of the State change.

Article 33 – Compliance with the Clean Air Act and Federal Water Pollution Control Act

Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 U.S.C. §§ 7401–7671q) and the Federal Water Pollution Control Act, as amended (33 U.S.C. §§ 1251–1387), when this Agreement is funded in whole or in part with federal funds and the total value of the Agreement exceeds one hundred fifty thousand dollars ($150,000). Contractor shall promptly report any violations to MDES and to the appropriate Regional Office of the Environmental Protection Agency. Compliance with these federal environmental requirements is a material condition of this Agreement.

Article 34 - Contractor Personnel

The Agency shall, throughout the life of the contract, have the right of reasonable rejection and approval of staff or subcontractors assigned to the work by Contractor. If the Agency reasonably rejects staff or subcontractors, Contractor must provide replacement staff or subcontractors satisfactory to the Agency in a timely manner and at no additional cost to the Agency. Such reasonable rejections shall include but are not limited to individuals who owe more than one week of unemployment insurance overpayments and individuals who have previously worked for MDES as an employee or as a temporary worker who are not eligible for rehire or reassignment. The day-to-day supervision and control of Contractor's employees and subcontractors is the sole responsibility of Contractor.

Article 35 – Debarment, Suspension, and Anti-Lobbying Requirements

Contractor certifies to the best of its knowledge and belief, that it:

1. is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency or any political subdivision or agency of the State of Mississippi;

2. has not, within a three-year period preceding this bid, been convicted of or had a civil judgment rendered against it for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state, or local) transaction or contract under a public transaction;
3. has not, within a three-year period preceding this bid, been convicted of or had a civil judgment rendered against it for a violation of federal or state antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
4. is not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, state, or local) with commission of any of the offenses enumerated in paragraphs (2) and (3) of this certification; and
5. has not, within a three-year period preceding this bid, had one (1) or more public transactions (federal, state, or local) terminated for cause or default.

Contractor further acknowledges that this Agreement may be funded in whole or in part with federal funds and agrees that no contract award may be made to parties listed on the government-wide exclusions maintained in the System for Award Management ("SAM") in accordance with 2 C.F.R. Part 180, as adopted and supplemented by the U.S. Department of Labor at 2 C.F.R. Part 2998, and Executive Orders 12549 and 12689. Contractor certifies that it is not presently listed as debarred, suspended, ineligible, or otherwise excluded in SAM and shall immediately notify MDES if its status changes. Compliance with these federal debarment and suspension requirements is a material condition of this Agreement.

If this Agreement exceeds one hundred thousand dollars ($100,000), Contractor also certifies, to the best of its knowledge and belief, that no federally appropriated funds have been paid or will be paid to any person or organization for the purpose of influencing or attempting to influence an officer or employee of any federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract or grant related to this Agreement, in accordance with the Byrd Anti-Lobbying Amendment (31 U.S.C. §1352). Contractor shall disclose any lobbying with non-federal funds as required by federal law and shall submit any required disclosures using Standard Form LLL, "Disclosure of Lobbying Activities." Contractor shall include the substance of this paragraph in all subcontracts exceeding one hundred thousand dollars ($100,000).

Article 36 - Disclosure of Confidential Information

In the event that either party to this agreement receives notice that a third party requests divulgence of confidential or otherwise protected information and/or has served upon it a subpoena or other validly issued administrative or judicial process ordering divulgence of confidential or otherwise protected information that party shall promptly inform the other party and thereafter respond in conformity with such subpoena to the extent mandated by law. This section shall survive the termination or completion of this agreement. The parties agree that this section is subject to and superseded by Mississippi Code Annotated §§ 25-61-1 et seq.

Article 37 - Exceptions to Confidential Information

Contractor and the State shall not be obligated to treat as confidential and proprietary any information disclosed by the other party ("disclosing party") which:

(1) is rightfully known to the recipient prior to negotiations leading to this agreement, other than information obtained in confidence under prior engagements;

(2) is generally known or easily ascertainable by nonparties of ordinary skill in the business of the customer;

(3) is released by the disclosing party to any other person, firm, or entity (including governmental agencies or bureaus) without restriction;

(4) is independently developed by the recipient without any reliance on confidential information;
(5) is or later becomes part of the public domain or may be lawfully obtained by the State or Contractor from any nonparty; or,

(6) is disclosed with the disclosing party's prior written consent

Article 38 - Failure to Deliver

In the event of failure of Contractor to deliver services in accordance with the contract terms and conditions, the Agency, after due oral or written notice, may procure the services from other sources and hold Contractor responsible for any resulting additional purchase and administrative costs. This remedy shall be in addition to any other remedies that the Agency may have.

Article 39 - Failure to Enforce

Failure by the Agency at any time to enforce the provisions of the contract shall not be construed as a waiver of any such provisions. Such failure to enforce shall not affect the validity of the contract or any part thereof or the right of the Agency to enforce any provision at any time in accordance with its terms.

Article 40 - Final Payment

Upon satisfactory completion of the work performed under this contract, as a condition before final payment under this contract, or as a termination settlement under this contract, Contractor shall execute and deliver to the Agency a release of all claims against the State arising under, or by virtue of, the contract, except claims which are specifically exempted by Contractor to be set forth therein. Unless otherwise provided in this contract, by state law, or otherwise expressly agreed to by the parties in this contract, final payment under the contract or settlement upon termination of this contract shall not constitute waiver of the State's claims against Contractor under this contract.

Article 41 - Force Majeure

Each party shall be excused from performance for any period and to the extent that it is prevented from performing any obligation or service, in whole or in part, as a result of causes beyond the reasonable control and without the fault or negligence of such party and/or its subcontractors. Such acts shall include without limitation acts of God, strikes, lockouts, riots, acts of war, epidemics, governmental regulations superimposed after the fact, fire, earthquakes, floods, or other natural disasters ("force majeure events"). When such a cause arises, Contractor shall notify the State immediately in writing of the cause of its inability to perform, how it affects its performance, and the anticipated duration of the inability to perform. Delays in delivery or in meeting completion dates due to force majeure events shall automatically extend such dates for a period equal to the duration of the

delay caused by such events, unless the State determines it to be in its best interest to terminate the agreement.

Article 42 - Indemnification

To the fullest extent allowed by law, Contractor shall indemnify, defend, save and hold harmless, protect, and exonerate the agency, its commissioners, board members, officers, employees, agents, and representatives, and the State of Mississippi from and against all claims, demands, liabilities, suits, actions, damages, losses, and costs of every kind and nature whatsoever including, without limitation, court costs, investigative fees and expenses, and attorney's fees, arising out of or caused by Contractor and/or its partners, principals, agents, employees and/or subcontractors in the performance of or failure to perform this agreement. In the State's sole discretion, Contractor may be allowed to control the defense of any such claim, suit, etc. In the event Contractor defends said claim, suit, etc., Contractor shall use legal counsel acceptable to the State. Contractor shall be solely responsible for all costs and/or expenses associated with such defense, and the State shall be entitled to participate in said defense. Contractor shall not settle any claim, suit, etc. without the State's concurrence, which the State shall not unreasonably withhold.

Article 43 - Independent Contractor Status

Contractor shall, at all times, be regarded as and shall be legally considered an independent contractor and shall at no time act as an agent for the State. Nothing contained herein shall be deemed or construed by the State, Contractor, or any third party as creating the relationship of principal and agent, master and servant, partners, joint ventures, employer and employee, or any similar such relationship between the State and Contractor. Neither the method of computation of fees or other charges, nor any other provision contained herein, nor any acts of the State or Contractor hereunder creates or shall be deemed to create a relationship other than the independent relationship of the State and Contractor. Contractor's personnel shall not be deemed in any way, directly or indirectly, expressly or by implication, to be employees of the State. Neither Contractor nor its employees shall, under any circumstances, be considered servants, agents, or employees of the Agency, and the Agency shall be at no time legally responsible for any negligence or other wrongdoing by Contractor, its servants, agents, or employees. The Agency shall not withhold from the contract payments to Contractor any federal or state unemployment taxes, federal or state income taxes, Social Security tax, or any other amounts for benefits to Contractor. Further, the Agency shall not provide to Contractor any insurance coverage or other benefits, including Worker's Compensation, normally provided by the State for its employees.

Article 44 - Modification or Renegotiation

This agreement may be modified only by written agreement signed by the parties hereto. The parties agree to renegotiate the agreement if federal and/or state revisions of any applicable laws or regulations make changes in this agreement necessary.

Article 45 - No Limitation of Liability

Nothing in this agreement shall be interpreted as excluding or limiting any liability of the Contractor for harm arising out of the Contractor's or its subcontractors' performance under this agreement.

Article 46 - Notices

All notices required or permitted to be given under this agreement must be in writing and personally delivered or sent by certified United States mail, postage prepaid, return receipt requested, to the party to whom the notice should be given at the address set forth below. Notice shall be deemed given when actually received or when refused. The parties agree to promptly notify each other in writing of any change of address.

For MDES:

Dr. William J. Ashley
Executive Director
Mississippi Department of Employment Security
1235 Echelon Parkway
Jackson, MS 39213

For Contractor:

Article 47 - Ownership of Documents and Work Papers

Agency shall own all documents, files, reports, work papers and working documentation, electronic or otherwise, created in connection with the project which is the subject of this agreement, except for Contractor's internal administrative and quality assurance files and internal project correspondence. Contractor shall deliver such documents and work papers to Agency upon termination or completion of the agreement. The foregoing notwithstanding, Contractor shall be entitled to retain a set of such work papers for its files. Contractor shall be entitled to use such work papers only after receiving written permission from Agency and subject to any copyright protections.

Article 48- Quality Control

Contractor shall institute and maintain throughout the contract period a properly documented quality control program designed to ensure that the services are provided at all times and in all respects in accordance with the contract. The program shall include providing daily supervision and conducting frequent inspections of Contractor's staff and ensuring that accurate records are maintained describing the disposition of all complaints. The records so created shall be open to inspection by the Agency.

Article 49 - Record Retention and Access to Records

Provided Contractor is given reasonable advance written notice and such inspection is made during normal business hours of Contractor, the State or any duly authorized representatives shall have unimpeded, prompt access to any of Contractor's books, documents, papers, and/or records which are maintained or produced as a result of the project for the purpose of making audits, examinations, excerpts, and transcriptions. All records related to this agreement shall be retained by Contractor for three (3) years after final payment is made under this agreement and all pending matters are closed; however, if any audit, litigation or other action arising out of or related in any way to this project is commenced before the end of the three-year period, the records shall be retained for one (1) year after all issues arising out of the action are finally resolved or until the end of the three-year period, whichever is later.

Article 50 - Recovery of Money

Whenever, under the contract, any sum of money shall be recoverable from or payable by Contractor to the Agency, the same amount may be deducted from any sum due to Contractor under the contract or under any other contract between Contractor and the Agency. The rights of the Agency are in addition and without prejudice to any other right the Agency may have to claim the amount of any loss or damage suffered by the Agency on account of the acts or omissions of Contractor.

Article 51 - Right to Audit

Contractor shall maintain such financial records and other records as may be prescribed by the Agency or by applicable federal and state laws, rules, and regulations. Contractor shall retain these records for a period of three years after final payment, or until they are audited by the Agency, whichever event occurs first. These records shall be made available during the term of the contract and the subsequent three-year period for examination, transcription, and audit by the Mississippi State Auditor's Office, its designees, or other authorized bodies.

Article 52 - Right to Inspect Facility

The State may, at reasonable times, inspect the place of business of a Contractor or any subcontractor which is related to the performance of any contract awarded by the State.

Article 53 - Severability

If any part of this agreement is declared to be invalid or unenforceable, such invalidity or unenforceability shall not affect any other provision of the agreement that can be given effect without the invalid or unenforceable provision, and to this end the provisions hereof are severable. In such event, the parties shall amend the agreement as necessary to reflect the original intent of the parties and to bring any invalid or unenforceable provisions in compliance with applicable law.

Article 54 - State Property

Contractor will be responsible for the proper custody and care of any state-owned property furnished for Contractor's use in connection with the performance of this agreement. Contractor will reimburse the State for any loss or damage, normal wear and tear excepted.

Article 55 -Third Party Action Notification

Contractor shall give the customer prompt notice in writing of any action or suit filed, and prompt notice of any claim made against Contractor by any entity that may result in litigation related in any way to this agreement.

Article 56 - Unsatisfactory Work

If, at any time during the contract term, the service performed or work done by Contractor is considered by the Agency to create a condition that threatens the health, safety, or welfare of the citizens and/or employees of the State of Mississippi, Contractor shall, on being notified by the Agency, immediately correct such deficient service or work. In the event Contractor fails, after notice, to correct the deficient service or work immediately, the Agency shall have the right to order the correction of the deficiency by separate contract or with its own resources at the expense of Contractor.

Article 57 - Waiver

No delay or omission by either party to this agreement in exercising any right, power, or remedy hereunder or otherwise afforded by contract, at law, or in equity shall constitute an acquiescence therein, impair any other right, power or remedy hereunder or otherwise afforded by any means, or operate as a waiver of such right, power, or remedy. No waiver by either party to this agreement shall be valid unless set forth in writing by the party making said waiver. No waiver of or modification to any term or condition of this agreement will void, waive, or change any other term or condition. No waiver by one party to this agreement of a default by the other party will imply, be construed as or require waiver of future or other defaults.

Article 58 - Requirements Contract

During the period of the contract, Contractor shall provide all the service described in the contract. Contractor understands and agrees that this is a requirements contract and that the Agency shall have no obligation to Contractor if no services are required. Any quantities that are included in the scope of work reflect the current expectations of the Agency for the period of the contract. The amount is only an estimate and Contractor understands and agrees that the Agency is under no obligation to Contractor to buy any amount of the services as a result of having provided this estimate or of having any typical or measurable requirement in the past. Contractor further understands and agrees that the Agency may require services in an amount less than or in excess of the estimated annual contract amount and that the quantity actually used, whether in excess of the estimate or less than the estimate, shall not give rise to any claim for compensation other than the total of the unit prices in the contract for the quantity actually used.

Article 59 - Change in Scope of Work

MDES may order changes in the work consisting of additions, deletions, or other revisions within the general scope of the contract. No claims may be made by Contractor that the scope of the project or of Contractor's services has been changed, requiring changes to the amount of compensation to Contractor or other adjustments to the contract, unless such changes or adjustments have been made by written amendment to the contract signed by MDES and Contractor. If Contractor believes that any particular work is not within the scope of the project, is a material change, or will otherwise require more compensation to Contractor, Contractor must immediately notify MDES in writing of this belief. If MDES believes that the particular work is within the scope of the contract as written, Contractor will be ordered to and shall continue with the work as changed and at the cost stated for the work within the contract.

Article 60 - Contract Management

If the Contractor fails to adhere to the services schedule, or if the Contractor fails to satisfactorily provide the prescribed service to all or any service area, MDES will inform the Contractor, and the Contractor shall complete corrective action within twenty-four (24) hours. No payment shall be made to the Contractor until all deficiencies have been corrected. If the Contractor exhibits a pattern of non-performance as shown by repeated deficiencies, MDES may terminate the contract without further obligation to the Contractor.

Article 61 - Insurance

The successful contractor shall maintain at least the minimum level of workers' compensation insurance, comprehensive general liability or professional liability insurance, with minimum limits of

$1,000,000.00 per occurrence and fidelity bond insurance with minimum limits of $100,000.00. All workers' compensation, comprehensive general liability, professional liability, and fidelity bond insurance will provide coverage to MDES as an additional insured. The Agency reserves the right to request from carriers, certificates of insurance regarding the required coverage. All insurance policies shall be issued by companies authorized to do business under the laws of the State of Mississippi, meaning insurance carriers must be licensed or hold a Certificate of Authority from the Mississippi Department of Insurance.

For the faithful performance of the terms of this contract, the parties hereto have caused this contract to be executed by their undersigned authorized representation.

MISSISSIPPI DEPARTMENT
OF EMPLOYMENT SECURITY

By: _____ By: _____

Dr. William J. Ashley
Executive Director

Date: _____ Date: _____

Exhibit A
SCOPE OF WORK

Contractor will provide Printing and Mailing Services including printing, sorting, folding, inserting, and mailing along with return mail processing services. The vendor shall quickly accommodate change requests to pull correspondences that MDES determines should not be mailed for reasons determined by the agency. The requested services must meet rigorous quality standards and specific timelines standards along with developing new processes to create more efficient and effective methods to meet the agency's printing and postal needs.

Scalability:

Contractor shall scale services to accommodate an increase or decrease in demands on an as-needed basis without disrupting processing.

General Requirements:

Contractor shall accept printing files ranging from raw data feeds to proprietary formats such as Adobe PDF. Contractor will include available and acceptable formats for print services as part of their submission document. Contractor will be able to advise MDES regarding opportunities to improve on existing print and mailing processes. MDES is seeking to automate many processes currently undertaken in manual efforts through the consolidation of services with a modern, well designed work flow. Contractor must be able to meet mailing service levels as determined by requirements generated by MDES requests

MDES prints include Forms, Reports, and On Demand ad hoc Prints including: Stuffers, Labels, Calendars, Catalogs, Guides, Brochures and Booklets. Both black and white as well as color printing formats are required. Contractor must be able to print, secure, and mail Unemployment Insurance checks when required.

Contractor will provide a Project Manager and any additional staff at no cost to the State, required for the analysis and implementation phases of the transition of services.

Contractor must provide programming services to meet or exceed current MDES printing and mailing services using application data files.

During the Start-up Phase, Contractor, at no cost to MDES, will print and mail PDF files for testing purposes. User acceptance testing (UAT) of services will be incorporated into the conversion and delivery process plan.

Contractor will provide custom programming, consultation and design services for all the print jobs using current process flows or future process flow requirements. Contractor should describe in detail including process flow diagrams, how our data files will be received and verified as well as how they will be processed once they have been received. This should also include file format requirements (processing time frames when relevant), a detailed outline for the process of document composition and mail processing.
During the Start-up Phase, all work must be completed (programming, printing, inserting, testing, mailing, etc.) approval before the contract start.
Contractor will provide a detailed Project Work Plan that will include but not be limited to the following:

Implementation and Post Implementation

Contractor will appoint a customer relationship manager in their organization to coordinate all implementation and post implementation activities, who will be the one point of contact for all communication.

Printing:

Contractor must print, fold and stuff inserts when applicable. With very few exceptions, all of these must be mailed out the same day or on an allotted schedule as agreed to by both parties. If Contractor is unable to meet the schedule requirements and work is not printed and mailed on the schedule, due to service provider issues, MDES will not incur related processing fees

Contractor will provide an online portal that will allow MDES access to all print jobs. The online portal can be used to proof read forms/reports. The portal must be searchable and would allow MDES to print or email individual documents should the need arise. The print files must be available on the portal no later than the day the forms are mailed. This portal should be designed to allow MDES to identify workflow roles and assign employees certain tasks by role.

Contractor will provide versioning history for all documents resulting from the print jobs at a record keeping level to be determined during contract phase. All versions kept should be accessible / searchable via the customer portal. This is in accordance to comply with Freedom of Information Act (FOIA).

The portal or an alternative framework will allow for dynamic messaging to be added to existing print materials utilizing existing whitespace on the document format. This dynamic messaging feature will eliminate creating separate informational documents and lower the cost of mailing to MDES.

Contractor must be able to create, proof, and print ad hoc forms and reports upon MDES request and complete the tasks on the same business day. Contractor may set submission timelines to accommodate the rapid turnaround of MDES requests.

Contractor will provide email or customer portal notification to MDES on the date the forms are mailed indicating how many prints were printed and mailed, and how many forms/reports were not printed due to any errors. Bidder submission documents may include other suggestions for verification processes to define level of service and verify task completion. During the contracting phase, Contractor and the department will incorporate language related to levels of performance as well as the reporting format.
Contractor will be accountable and will manage inventory of materials for contracted print and mail services. Contractor must procure and store all printing stock, envelopes and related supplies. They will also manage storage and mailing of any preprinted materials such as forms and booklets.

Mailing: Outbound and Inbound processing

Contractor must disclose the discounted postal rate(s), and the percent of forms that will be mailed at that rate. Contractor must guarantee the lowest postal rates allowed by the Postal Service, provide current rate schedules and conditions or additional fees which apply, and indicate price points for reduced cost of services and method of calculation for accrued services to meet price points.

Mailing guidelines exist to determine the number of days for delivery for certain types of documents based on geographic location from the state government offices and range from next

day delivery to 3-day delivery. These requirements will be defined during a contracting phase with Contractor.

Contractor must show the appropriate level of insert capabilities, such as sorting, folding, and inserting by recipient or by address to identify opportunities for group correspondence and consolidated mailings by type.

Contractor will provide access to production reports via a portal displaying all bad addresses. Contractor will provide access to an output file which the MDES benefit system will use to correct bad addresses via agreed upon business rules. Contractor will be CASS certified, and scrub for bad addresses. Please provide evidence of CASS software and US Postal certification in your submission.

Contractor must have the ability upon request to track a piece of mail to the point where it is handed off to the mail carrier.

Contractor must print 2D barcode on all automated forms containing recipient information for purposes of tracking and verification of process integrity.

Contractor should provide pricing for inbound mail processing and return mail processing. They should have the ability to receive all returned mail daily, scan and upload them to a portal for MDES review. Customer portal function must include ability to sort and pre-assign work by service process type, department or by individual recipient depending on the subject matter.

Contractor must process Canadian and foreign mail services.

Contractor will provide a description of the process used to track and charge postal rates based on overall volume on a monthly or other agreed upon process which provides the greatest benefit of accumulative volume pricing to MDES.

Contractor must adhere to the postal addressing standards outlined in the below URL http://pe.usps.gov/text/pub28/welcome.htm

Security and Business Continuity:

Contractor must provide a means for secure data transmission and confirm receipt of the Department's data and files. Contractor must accept and receive File Transfer Protocol Secure transmissions to ensure secure data exchanges. For the purposes of disaster recovery and business continuity, Contractor must have access to a dedicated 24/7/365 restoration process that offers full restoration and recovery of services within 24 hours or agreed upon Shared-Loss Agreement standards. Contractor must also provide the business continuity plan illustrating redundancies in existing facilities and equipment to ensure continuous operations and high availability of services.

Contractor must provide a copy of their most recent SSAE 16 Audit Report, other third-party assessments and copy of business continuity/disaster recovery plan for printing, mailing and computing.

Contractor will provide a copy of its security policy and testing procedures which Contractor and all its subcontractors must meet that conforms to all State of Mississippi and Federal security guidelines for the handling of financial and personal identifying information data, including all confidentiality statutes specific to the Unemployment Insurance program. These requirements

include State of Mississippi and IRS security standards for handling Federal Tax Information ("FTI") and Personally Identifiable Information ("PII") data.

Contractor must supply proof of employee background checks to meet State and Federal materials handling standards.

Contractor must supply proof of mailing process security standards to ensure that no information is mishandled or misdirected due to gaps in chain of custody or control of material issues.

Any subcontractor utilized by Contractor must meet these same standards, and Contractor is accountable for providing documentation on request.

Billing and Documentation:

Contractor must invoice MDES monthly for billable services provided the previous month. The invoice format must be acceptable to MDES; including a summarized breakdown of the number of prints mailed at each discounted postal rate, including the beginning and ending balance.

The above information needs to be subtotaled (separated) by copies/printing or postage. These items can be billed on the same invoice, but the service (postage or copies) quantities and cost must be subtotaled.

This will allow MDES to differentiate service charges and to properly apply object codes. Contractor needs to have the capability to identify the service provided, determine which bureau it belongs to, and to append the correlating charge coding for funding for each service provided that month.

The invoice format and billing capabilities should be able to accommodate "split billing." Central Print jobs that require "split billing" is captured by document name/type and charge code. If there are two separate entities, the billing system is required to: (a) allocate the respective percentages' towards each document type, (b) split the bills as per the percentage allotted by the funding entities. Upon payment of the invoice, the service center handling the accounts payable process should be able to assign the correct funding account code to the monthly printing and postal cost for the specific document type. The Advantage. Supporting documentation may be required to determine the correct fund accounting code by document name/type.

Other Services

Contractor must provide:

- Services and pricing for PDF generation and upload of documents to searchable customer portal;

- Services and pricing for new form generation;

- Services and pricing for a report generator via the portal with fixed reports and ad hoc report capabilities;

- Any additional portal hosting and storage costs to MDES;

- Services and pricing for return mail services. The supplier will receive all return mail daily, scan and upload them to a searchable portal for customer review and utilization;

- Services and pricing for inbound mail services. Contractor will receive all inbound mail daily, scan and upload these documents to a searchable portal for customer review and utilization. Mailing guidelines exists to determine the number of days for servicing inbound documents based on geographic location from the state government offices and range from next day to 3-day delivery servicing. These requirements will be defined during a contracting phase with Contractor

- Agreed upon verification quality assurance and audit process ensuring the quality, the printing and mailing services. This process will detail the methodology for error tracking including options for resolution or mitigation of errors. Contractor will provide monthly reports containing quality assurance metrics

Portal Functions

Contractor should provide the following functions for the customer porter to meet the minimum requirements:

- Provide MDES access to all print jobs;

- Proof read new forms/reports before they are moved to production;

- Allow for dynamic messaging to be added to existing print materials;

- Customer portal notification indicating how many items were printed and mailed, and how many forms/reports were not printed due to any errors

- Provide an option to display bad addresses;

- Provide the ability to sort and pre-assign work (workflow) by service process type, department, or by individual recipient depending on the subject matter for inbound and return mail; and,

Provide the ability to scan, upload mail (inbound and return mail), search and print forms/reports via the portal.

Exhibit B
AI Governance Policy

PURPOSE: The purpose of this policy is to establish a set of standards, procedures, and guidelines which govern the requisition and implementation of Artificial Intelligence within the Mississippi Department of Employment Security (MDES technological environment. As AI continues to expand its presence within modern enterprise environments, MDES has begun to consider expansion of its offerings to include platforms and applications which leverage automation to improve scalability and decrease reliance upon human interaction with end users. MDES recognizes the necessity that any automation leveraging AI must be implemented responsibly and ethically, and that AI is a complement to its existing human-based services, as opposed to a replacement.

DEFINITIONS:

Artificial Intelligence (AI): Artificial Intelligence (AI) -has the meaning set forth in 15 U.S.C. §9401(3) (section 5002(3) of Pub. L. 116-283) that states "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

Convolutional Neural Networks (CNN): Convolutional Neural Networks are a subset of Machine and Deep Learning that utilizes convolutional layers to analyze and classify images and recognize objects within them. CNNs are primarily focused on image recognition and identification.

Deep Learning (DL): Deep Learning is a subset of Machine Learning (ML) that utilizes multilayered neural networks to simulate complex decision-making including image recognition, natural language processing, and speech recognition. Deep learning focuses on prediction and classification.

Foundation Model (FM): A foundation model is a large Machine- Learning model that forms the foundation for many downstream tasks and applications. Large foundation models are pre-trained on massive amounts of data and require a lot of computing to build. This allows them to learn vast amounts of knowledge and

patterns. The FM can then be fine-tuned for specific tasks like language translation, text summarization, image recognition, or domain-specific purposes.

Generative Artificial Intelligence (GenAI): Generative AI refers to AI that is capable of and used to produce new content, including, audio, code, images, text, and video, according to the data inputs and machine learning model on which it is trained. This type of AI can create the same content when prompted by a user. GenAI may include both Large Language Models (LLM) and other types of ML models to allow them to perform two functions: (1) to perform the tasks of a LLM and also (2) to analyze images and recordings, or create similar items in response to prompts from a user. GenAI requires training to focus on the creation of new content.

Large Language Model (LLM): A Large Language Model is a type of AI model specifically designed to process and generate human language. LLMs are trained on vast amounts of text data, enabling them to understand, generate, and translate text, as well as answer questions and perform other language-related tasks.

Machine Learning (ML): Machine Learning is a subset of AI that involves the development of algorithms and models that enable computers to learn from and make predictions or decisions based on data. Rather than being explicitly programmed for specific tasks, ML systems identify patterns within data and use those patterns to improve their performance over time.

Natural Language Processing (NLP): Natural Language Processing is a type of AI model specifically designed to understand and process human language, written and spoken. NLPs utilize structure rules to translate analyze, and manipulate human language to compute, extract, and perform tasks related to language.

Robotic Processing Automation BOT (RPA BOT): Robotic Processing Automation BOTS are software robots that perform specific tasks based on user-defined rules and workflows. The following characteristics distinguish RPA BOTs: they require human intervention to make decisions and to adapt to new information; they are incapable of "learning", and they are not designed for autonomy.

OBJECTIVES:

This policy is designed to ensure that the integration of AI into MDES assets, processes, and offerings is governed via an enforceable set of standards and guidelines which define responsible use, the safeguarding of data proprietary to the agency and its end users, and ethical standards relevant to any existing or future AI-based projects.

SCOPE: This policy shall be applied to all internal implementations of AI within MDES, and, by extension, any business partner or third-party vendor from which this agency procures technologies that employ AI or support for such products and services.

This policy shall not be applied to internal implementations of RPA BOTs. Essentially, RPA BOTs follow strict instructions provided by human programming. These AI applications do not analyze complex information, learn from data, or make

autonomous decisions in dynamic situations without human intervention. RPA BOTs must be reviewed to determine if any special functions such as analysis, learning, or autonomous decision-making are being utilized, that would require the application of this policy.

The only authorized AI tools are LLMs, CNNs, DLs, LLMs, MLs, or, NLPs, or any other later-developed AI tools. These AI tools must have been developed in the United States, by entities authorized to do business in the United States, or be approved for use by the MDES Executive Committee after a description of the AI from the AI Officer.

ROLES AND RESPONSIBILITIES:

Formal designations shall be established and documented which define authorities within MDES responsible for the execution, review, and maintenance of this policy. This shall include the following:

1. **AI Officer** (or equivalent as defined by MDES): This person shall provide oversight of AI governance, ensuring all delegated roles are performing their responsibilities effectively. This shall include:
   A. Planning with Agency Executives to develop strategic decisions related to AI governance, ethical alignment, and regulatory compliance.
   B. Leading and coordinating the AI governance team, ensuring collaboration and alignment with organizational goals.
   C. Serving as the authoritative voice in AI project approvals, policy updates, and key decisions. Preparing high-level reports for senior management and the Executive Director.
   D. Overseeing the collection, preparation, and management of data used in the AI system, ensuring data quality, consistency, and readiness for AI processes.
   E. Providing guidance and engaging with senior management to aid in the procurement of AI services and products.
   F. Coordinating the revision of this AI policy if the Governor's executive order, state or federal law or regulations affect or nullify any provisions herein.

2. **AI Governance Team**: A designated group of staff which report to the AI Officer will be responsible for the day-to-day management and operational support of AI systems within the organization. The team's key responsibilities include: Managing the setup, integration, and ongoing maintenance of the AI application.
   A. Continuously monitoring the AI model's performance and troubleshooting any technical issues that arise.
   B. Engaging with the AI Officer to conduct regular reviews of AI integration and implementation within the MDES environment.
   C. Providing training to staff regarding this AI policy and staff interactions with each specific integrated AI application.

D. Developing a process to identify potential use cases to capture common problems and scenarios where AI can be used beneficially. Also, maintaining a use case inventory of these identified use cases.
E. Establishing and updating a methodology for the prioritization and review of the AI use cases to include, but not be limited to, factors such as potential cost savings, improved service delivery, enhanced customer experience, improved staff quality of life, and increased efficiencies.

The above listed AI Officer and AI Governance Team may be hired to exclusively perform this role or be existing staff who have been designated by the Executive Director or his designee to perform this role.

INTERNAL AI GOVERNANCE:

MDES recognizes that although AI integration into its current services will aid in expediting and automating its customer service experience, the sensitive nature of client data the agency collects, transmits, and stores must be considered and safeguarded at all times.

MDES has taken the steps necessary to identify data which falls within the purview of the relevant compliance standards including IRS 1075 and NIST 800-171. To ensure that current and future AI integration does not undermine technical and administrative controls as well as any executive order, state or federal law or regulations currently imposed or later issued, enacted, promulgated, or adopted on sensitive data within the MDES environment, the following standards must be adhered to:

1. **Data Protection**: Any integration of AI services and products provided by third-party vendors must not interact with sensitive data in any capacity:

A. AI technologies managed or supported by an external party must not be provided any sensitive data unless the vendor provides specific safeguards designed for utmost security for data used in artificial intelligence applications. This shall include sharing of sensitive data with the vendor itself, or importing sensitive data into a language model supported, managed, or provided by a third-party vendor.

B. Sensitive data shall be defined as staff and customer personal identifiable information (PII), Federal Tax Information (FTI), and/or any data governed by the legal standards in section 1(f) above.

C. Integration of sensitive data into a LLM or other AI repository effectively renders the entirety of the model as sensitive through sensitivity inheritance. This must be avoided where possible and secured using the highest-level safeguards available to ensure the protection of the data.

2. **Monitoring**: All AI integration within the MDES environment and its services will be continuously monitored to ensure data accuracy and integrity. A required component of modern AI integration involves human oversight of results generated by machines.

   a. Appropriate baselines must be established, documented, and regularly reviewed for all AI services. This shall include metrics such as data throughput, processing time, and input sanitization to include responses to malicious prompts.
   b. A member of the AI Governance team shall be tasked with consistent monitoring of all AI applications, services, and products. This will include systematic "spot checking" at defined intervals to identify the following:
      1. Algorithm deviation
      2. Unintended responses derivative of a LLM (hallucination)
      3. Exposure or introduction of sensitive data
      4. Tracking and moderation of undesirable and/or harmful content.

3. **Reporting**: Any perceived or realized importation of sensitive data to a third-party managed AI service or product must be reported immediately:

   a) All staff must be aware of a requirement to alert the AI Officer in the event of a perceived or realized disclosure of sensitive data immediately.
   b) The AI Officer will work with appropriate staff to determine whether an incident has occurred.
   c) If it is determined that an incident has occurred, the AI Officer will coordinate with relevant staff to initiate the agency's AI Incident Response plan.

4. **Human Oversight**: Human oversight and intervention must be maintained at all times as AI solutions are requisitioned, installed, and employed within the MDES environment.

   a) AI systems should not be solely responsible for making critical decisions without human intervention. Important decisions, particularly those impacting sensitive data or significant agency operations, must involve human review and approval.
   b) Human oversight is necessary to validate and interpret AI-generated outcomes, ensuring they align with organizational goals and ethical standards.
   c) Integration of AI into MDES' current offerings is intended to complement or enhance human-designed and managed services. AI should be leveraged to support critical information system and business processes which are reliant upon

human interaction and intervention so long as the responsibility for a decision or final determination rests with an Agency staff person and not an AI application.

EXTERNAL AI GOVERNANCE:

MDES does not currently intend to develop AI, CNN, DL, LLM, ML, NLP platforms and applications internally. As such, the agency will rely upon a third-party vendor to procure and support the integration of AI functionality into its existing services. All external parties which MDES procures AI technology from are subject to the following:

1. **Disclosure of AI Tooling**: All vendors must acknowledge and disclose tooling necessary to the function of the requisitioned service to the extent that MDES understands how the tool handles its proprietary information.
    a) Any functions provided through a party external to the vendor must be disclosed prior to acquisition of the product or service.
    b) MDES understands the constraints of intellectual property (IP) considerations and all disclosures should balance necessary transparency and sensitive data issues with IP concerns of vendors.
2. **Isolation**: Any service that is managed or supported by an external entity to MDES and its network perimeter must ensure that any data exchanged between vendor and client is isolated physically or logically from other clients. Neither MDES data that is used to tune an FM utilized by the Agency or the tuned FM itself may be shared with model providers, or used to improve base models. FMs utilized by MDES should be private copies of the FM ensuring both physical and logical isolation of MDES data and tuning.

This shall include transmission, processing, and storage of any data proprietary to MDES beyond its network perimeter.

2. **Data Sharing**: Any intent or need to share data between the vendor and an external party aside from MDES must be disclosed prior to acquisition.

No data provided by MDES shall be transmitted or stored remotely by the vendor without expressed, documented permission from the Agency.

3. **Internal Control**: Vendor must make available to MDES a centralized platform with which to monitor the AI, LLM, or ML AI, CNN, DL, LLM, ML, NLP service whilst in use within the MDES environment.
    a) The platform must provide MDES the ability to control the AI environment, to include starting and stopping the service as needed.
    b) If the AI platform is considered an integral part of critical infrastructure or core business, then the vendor must provide MDES with a “kill switch” that will gracefully transfer control back to humans tasked with oversight.

4. **Regulatory Compliance**: In the event that a proposed AI project will interface directly or indirectly with any data which MDES manages, the vendor must ensure compliance with all relevant regulations and standards as imposed by the agency.

This includes adherence to legal requirements specific to data protection and privacy, ensuring that the vendor's practices align with MDES' compliance obligations.

DATA QUALITY AND INTEGRITY:

1. **Accuracy**: All vendors must develop processes in coordination with MDES that helps to ensure that the data used to train its AI systems is accurate and reflective of the real-world scenarios it aims to model. Any detected inaccuracies must be corrected promptly.
2. **Relevance**: All vendors must develop processes in coordination with MDES to help ensure that data used for the training of AI models is current, and to set the required intervals to refresh data sets to maintain their relevance. Outdated data that could affect decision-making or predictions must be identified and updated regularly.

All data used must be relevant to the specific AI application, ensuring that only necessary data is included to reduce noise and potential biases.

3. **Validation**: Regular validation of data must be conducted to identify and correct errors, anomalies, or inconsistencies. Vendors should utilize automated and manual validation techniques to ensure data accuracy.

4. **Auditing**: Periodic audits must be performed by vendors to assess the integrity of data throughout its lifecycle, from collection to processing and storage. Audit results should be shared with MDES to ensure transparency and accountability. The Vendor is encouraged to offer integrated and automatic audit functions.

RISK MITIGATION AND ASSESSMENT:

1. **Security Controls**: Vendors must implement robust security measures to protect sensitive data, including encryption, access controls, and regular security testing. These measures must align with MDES's internal security policies.

   Vendor must agree to employ security controls necessary to meet the expectations of the legal standards imposed on MDES for all data which it handles., be it technical, administrative, or physical.

2. **Data Handling**: Vendor must agree to and demonstrate the ability to employ data handling protocols commensurate with MDES' legal requirements. This includes the methods with which data is collected, stored, transmitted, and processed. These protocols must minimize the risk of unauthorized access or data breaches.

3. **Risk Assessments**: The integration of AI applications must be incorporated into MDES's existing Risk Assessment Plan. This includes identifying specific AI-related risks, such as model bias, data leakage, and system vulnerabilities, and developing strategies to mitigate these risks.

   Both MDES and vendors providing AI products or support must perform annual risk assessments of such integrations. These assessments should evaluate potential threats to data security, privacy, and ethical standards, as well as the effectiveness of existing controls.
4. **Training and Awareness**: To ensure effective risk management and mitigation, MDES will implement a comprehensive training program for all relevant staff and stakeholders.
   a) AI and Data Privacy Training shall be conducted annually for all senior management and staff which comprise AI Governance Team, including the AI Officer.
   b) Training course content will include an overview of AI technologies, data privacy principles, and specific legal standards that apply to the Agency's operations.

ETHICAL AI USE AND TRANSPARENCY:

MDES recognizes the need to ensure that any AI integration is designed to abide by certain ethical standards to avoid generating biased or otherwise harmful responses. As such, each vendor must agree to and comply with the following:

1. Vendors and MDES must ensure that any integrated AI applications respond to prompts fairly, without discriminating against individuals or groups based on characteristics such as race, gender, age, or religion.
2. The use of AI for activities that could cause physical, psychological, or social harm is strictly prohibited. This includes using AI for surveillance, profiling, or decision-making that negatively impacts individuals or communities without their informed consent. This requirement requires oversight to ensure the AI uses only legal methods of profiling and identification of information and any decision generated from said AI usage regarding a claimant or employer is made by an Agency staff person.
3. AI projects must undergo an ethical review process prior to implementation. This review will assess potential ethical risks and ensure that AI applications align with MDES's values and ethical standards.

Exhibit C

SSA Information Security and General Privacy Requirements

SSA INFORMATION SECURITY AND GENERAL PRIVACY REQUIREMENTS

1. Definitions

- **Authorization to Operate (ATO):** The official management decision given by a senior official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls.
- **Breach:** The loss of control, compromise, unauthorized disclosures, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses confidential information; or (2) an authorized user accesses or potentially accesses confidential information for an other than authorized purpose. This includes a breach in any medium or form, including paper, oral, and electronic. A breach is not limited to an occurrence where a person other than an authorized user potentially accesses confidential information by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include confidential information and portable electronic storage media that store confidential information, the inadvertent disclosure of confidential information on a public website, or an oral disclosure of confidential information to a person who is not authorized to receive that information. It may also include an authorized user accessing confidential information for other than an authorized purpose. Often, an occurrence may be first identified as an incident, but later identified as a breach once it is determined that the incident involves confidential information, as is often the case with a lost or stolen laptop or electronic storage device.
- **Confidential Information**: Information or data, or copies or extracts of information or data, that is: (1) provided by the Social Security Administration (SSA) to the Contractor for, or otherwise obtained by the Contractor in, performing work under this contract; and (2) of a personal nature about an individual, such as name, home address, and social security number; proprietary information or data submitted by or pertaining to an institution or organization, such as employee pay scales and indirect cost rates; sensitive information;

controlled unclassified information; Federal Tax Information; or information designated by SSA as confidential for other reasons. Confidential information includes all personally identifiable information (PII) provided by SSA to or collected or acquired by the Contractor as a result of this contract. Aggregations and tabulations of such PII, as well as de-identified individual-level data, shall also be treated as confidential information, unless SSA has provided written approval for public dissemination.

- **Controlled Unclassified Information (CUI)**: Non-classified information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
- **Federal Information:** Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.
- **Federal Information System:** An information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency. An information system that does not meet such criteria is a "nonfederal information system".
- **Federal Tax Information (FTI):** Information that SSA obtains from the Internal Revenue Service (IRS) or on behalf of IRS. FTI is also referred to as "tax return information" or "return information." FTI is governed by the Internal Revenue Code (IRC). The IRC defines "return information to include "a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over-assessments, or tax payments. 26 U.S.C. § 6103(b). FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable information (PII).
- **Federal Websites and Digital Services:** Federal agency public websites and digital services are defined as online information resources or services maintained in whole or in part by the departments and agencies in the Executive Branch of the U.S. Federal Government that are operated by an agency, Contractor, or other organization on behalf of the agency.
- **Incident:** An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- **Nonfederal Information System:** An information system that does not meet the criteria of a federal information system.

- **Personally Identifiable Information (PII)**: Information that can be used to distinguish or trace an individual ‘s identity, either alone or when combined with other information that is linked or linkable to a specific individual, such as medical, educational, financial, and employment information. PII includes, but is not limited to, names, Social Security numbers (SSNs) financial account numbers, birth dates, and biometrics identifiers (e.g. fingerprints and facial images). PII only includes information that is made or becomes available to the Contractor as a result of performing under this contract or provided by SSA.
- **Plan of Action and Milestone (POA&M):** A corrective action plan to track and resolve identified system security weakness.
- **Secure area** or **Secure duty station:** For the purpose of this clause, either of the following, unless the agency expressly states otherwise on a case-by-case basis: (1) a Contractor employee’s official place of work that is in the Contractor’s established business office in a commercial setting, or (2) a location within the agency or other Federal- or State-controlled premises, or (3) a remote work environment (when remote work is authorized by the agency. A person’s private home, even if it is used regularly as a “home office” (including that of a Contractor management official), shall not be considered a secure area or duty station.
- **Sensitive Information:** Information or data of which the loss, misuse, unauthorized access to, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled to under 5 U.S.C. § 552a (the Privacy Act), but which no Executive Order or Act of Congress has specifically authorized to be kept secret in the interest of national defense or foreign policy.
- **Suspected Breach:** An unconfirmed breach. See the definition of breach for more information.

2. Information Security and Privacy Governance

The Contractor shall comply with the laws, regulations, directives, policies, standards, and guidelines listed in *Appendix C - Attachment A*, as well as any applicable amendments published after the effective date of the contract. In all cases where this contract references federal guidance (including but not limited to SSA policies, OMB guidance and memorandums, and NIST guidance and publications), the Contractor shall comply with the most recently published, final version of that guidance. If such guidance is rescinded completely or there is a question about which version the Contractor must comply with, the Contractor shall seek clarification from the COR.

The Contractor shall confirm and attest compliance with SSA's information security and privacy requirements in this contract prior to award and shall maintain compliance with each requirement throughout the duration of the contract, through contract closure or termination.

3. Subcontractors

The Contractor shall include all privacy and security requirements in this contract in all resulting subcontracts whenever there is any indication that the subcontractor(s) and their personnel, or successor subcontractor(s) and their personnel, will or may perform work that would be subject to such requirements if performed by the Contractor. When a subcontract is awarded, all references to "Contractor" in all privacy and security requirements in this contract apply to subcontractor(s).

The Contractor shall retain operational configuration and control of any systems used to process and store federal information, including any systems used in remote work environments (when remote work is authorized by the agency). The Contractor shall not subcontract the operational configuration and control of any system used to process or store federal information.

Note: The subcontractor is required to notify the prime Contractor in instances where the language states the Contractor shall notify the agency or COR.

4. Indemnification

a. Indemnify the agency and its officers, agents, and employees acting for the agency against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of the Contractor's unauthorized introduction of copyrighted material, information subject to a right of privacy, and any libelous or other unlawful matter into federal information. The Contractor agrees to waive all defenses that may be asserted for its benefit, including (without limitation) the Contractor's Defense.

b. Indemnify the agency and its officers, agents, and employees acting for the agency against any liability arising out of the performance of this contract, including costs and expenses, incurred as the result of
    i. The Contractor's unauthorized disclosure of trade secrets, copyrights, Contractor bid or proposal information, source selection information, classified information, material marked "Controlled Unclassified

Information", information subject to a right of privacy or publicity, personally identifiable information or any record as defined in 5 U.S.C. § 552a; or

ii. The Contractor's unauthorized introduction of any libelous or other unlawful matter into federal information. The Contractor agrees to waive all defenses that may be asserted for its benefit, including without limitation the agency Contractors Defense.

c. In the event of any claim or suit against the agency on account of any alleged unauthorized disclosure or introduction of data or information arising out of the performance of this contract or services performed under this contract, the Contractor shall furnish to the agency, when requested by the CO, all evidence and information in the Contractor's possession pertaining to such claim or suit. Such evidence and information shall be furnished at the expense of the Contractor; provided, however, that an equitable adjustment shall be made under this clause, and the contract modified in writing accordingly, if the claim or suit is withdrawn, settled, or adjudicated in favor of the agency, and the basis for the claim or suit, regardless of outcome, was not due to any act or omission of the Contractor.

d. The provisions of this paragraph do not apply unless the agency provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to any libelous or other unlawful matter contained in such data furnished to the Contractor by the agency and incorporated in data to which this clause applies. Further, this indemnity shall not apply to:
    i. Disclosure or inclusion of data or information upon specific written instructions of the CO directing the disclosure or inclusion of such information or data;
    ii. Third-party claim that is unreasonably settled without the consent of the Contractor, unless required by final decree of a court of competent jurisdiction.

5. Safeguarding Federal Information and Information Systems

The Contractor shall:

a. Protect federal information and information systems to ensure:
    i. *Confidentiality*, which means preserving authorized restrictions on access and disclosure, based on the information security terms found in this contract, including means for protecting personal privacy and proprietary information;

    ii. *Integrity*, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and

    iii. *Availability*, which means ensuring timely and reliable access to and use of information.

b. Provide security for any information systems, and information contained therein, connected to an SSA network, or operated by the Contractor on behalf of SSA regardless of location. In addition, if the Contractor discovers new or unanticipated threats or hazards to such information systems, and information contained therein, or if existing safeguards to protect such systems and information have ceased to function, the Contractor shall immediately, within one (1) hour, bring the situation to the attention of the COR.
c. Adopt and implement the policies, procedures, controls, and standards, as provided by the COR, to ensure the confidentiality, integrity, and availability of federal information and federal information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract.

Comply with all applicable Privacy Act requirements and FAR and Agency Specific clauses included and referenced in this contract.

6. Information Security Categorization

The risk level for each security objective (confidentiality, integrity, availability) and the overall risk level, which is the highest watermark of the three security objectives of the information or information system, are the following:

Confidentiality:	[ ] Low	[ ] Moderate	[ ] High
Integrity:	[ ] Low	[ ] Moderate	[ ] High
Availability:	[ ] Low	[ ] Moderate	[ ] High
Overall Risk Level:	[ ] Low	[ ] Moderate	[ ] High

Note: This information security categorization reflects information provided by the Chief Information Security Officer, or other security representative, in accordance with Federal Information Processing Standards (FIPS) 199 and NIST SP 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix C.*

7. Personally Identifiable Information (PII)

Based on information provided by the security or privacy representative, the agency determined that this acquisition includes creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII:

[ ] No PII [ ] Yes PII

PII Confidentiality Impact Level has been determined to be:

[ ] Low [ ] Moderate [ ] High

8. Minimum Security Baseline

The Contractor shall ensure that all federal information systems or services it provides shall meet or exceed the minimum-security baseline corresponding to a ***[insert contract-specific impact level]*** -impact system under the latest revision of NIST Special Publication 800-53.

9. Controlled Unclassified Information (CUI)

[The Contractor must comply with Executive Order 13556, *Controlled Unclassified Information*, CUI Regulations at (32 CFR, Part 2002); the CUI Registry; and any successor order or regulations when handling CUI. The term "*handling*" refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 32 CFR § 2002.4(aa). The Contractor shall safeguard CUI consistent with 32 CFR § 2002.14 and requirements elsewhere in this contract. Misuse of CUI is subject to penalties established in applicable laws, regulations, and Government-wide policies and must be reported to the CO upon discovery. In safeguarding CUI all information shall be:

1. Marked appropriately;
2. Only disclosed to authorized personnel who have a need for the information in performance of duties under this contract;
3. protected in accordance with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, applicable baseline if handled by a Contractor on a federal information system operated on behalf of the agency.
4. Protected in accordance with NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, if handled by Contractor on a nonfederal system which has been explicitly approved for use by the CO or COR; and
5. Returned to SSA control or disposed of in accordance with the terms of this contract.

The agency determined that this acquisition includes creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of CUI:

a. [ ] No CUI [ ] Yes CUI
b. CUI Category (e.g. PII, FTI) [ ]

Note: Additional CUI categories may be identified or created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed as a result of or as part of this contract after the award of this contract and would be subject to this contract. For any questions about CUI, consult with the CO.

10. Protecting CUI on Nonfederal Information Systems

The Contractor shall not handle federal information with a nonfederal information system unless the CO or COR has explicitly approved such system for use (Authority to Operate (ATO)). The Contractor shall ensure that all nonfederal information systems, which the Contractor is responsible for, that process or store CUI meet or exceed the security controls as specified by NIST SP 800-171.The Contractor shall:

1. Develop policies and procedures to implement security controls and requirements as required by NIST 800-171.

2. Implement continuous monitoring processes to maintain ongoing awareness of nonfederal systems and related security process to ensure compliance with the security controls as required by NIST 800-171.

3. As requested by the COR, participate in Contractor security reviews, provide current documentation describing security controls, coordinate inspections, if the agency requests, and plan for and perform remediation activities to address weaknesses.

4. Ensure that CUI is returned, disposed, or destroyed in accordance with SSA requirements for termination of a contract.

11. Cybersecurity Supply Chain Risk Management

The Contractor is responsible for adhering to all applicable cybersecurity supply chain risk management requirements as outlined by federal regulations and agency policies. In accordance with EO 14028, the Contractor must implement robust cybersecurity practices to secure the supply chain, including the identification and mitigation of risks associated with the development, acquisition, and deployment of information and communications technology. Compliance with NIST 800-161 requires the Contractor to integrate cybersecurity supply chain risk management practices into their organizational processes, conduct thorough due diligence on their suppliers and subcontractors, and ensure that all products and services provided are free from known vulnerabilities and comply with established security standards. Additionally, the Contractor must:

- Implement safeguards to protect sensitive information.
- Cooperate fully with agency assessments and audits.

- Maintain transparency regarding the origin and integrity of hardware, software, and services.
- Notify the agency of any supply chain changes that could impact security.
- Participate in the Government's Continuous Cyber Risk Monitoring Program, including providing information and participating in regular risk posture reviews.
- Undergo a cybersecurity risk assessment via the Government's selected Cyber Risk Monitoring platform prior to contract award; assessment determines Contractor eligibility and risk management controls.
- Promptly report cybersecurity incidents or supply chain risks.
- Remediate identified cybersecurity risks within a specified timeframe, failure may result in corrective action, including contract remedies per FAR 52.212-4 and agency-specific protocols.

12. Privacy Assessments

The Contractor shall assist the agency with conducting a Privacy Assessment (such as a Privacy Threshold Analysis, or PTA; or Privacy Impact and Risk Assessment, or PIRA) for the information system or information handled under this contract as deemed necessary by the agency. The primary purpose of the Privacy Assessment is to ensure the information system, project, program, or information process complies with the Privacy Act. Specifically, the assessment reviews the information system against established privacy controls, such as a Privacy Impact Assessment (PIA), Privacy Act Statement, or Systems of Records Notice (SORN), and determines the privacy risk compliance or if privacy risk mitigation strategies, such as updates to those documents are necessary.
Assistance from the contractor will consist of providing documentation, such as, but not limited to a Business Process Description, messages on screens, privacy notices, screening tools, and email or text communication.

1. If the agency's privacy assessment determination finds that a new or modified PIA is needed, the Contractor shall assist the agency with completing documentation required for the system or information. The Contractor shall provide documentation or information needed to complete this process within a timeframe agreed upon with the COR, but no later than ***/insert contract specific timelines/*** days after the documentation or information has been requested by the COR.
2. The Contractor shall assist the COR or designee in reviewing the privacy assessment at least every [***insert contract-specific timeline***] throughout the system development lifecycle/information lifecycle, or when the agency

determines that a review is required based on a major change to the system, when the system processes new information types, or when the system introduces new or increased privacy risks, whichever comes first.

13. Digital Identity Risk Assessment (DIRA)

The Contractor is required to adhere to requirements in the latest version of NIST SP 800-63.

The Contractor shall assist SSA with conducting a Digital Identity Risk Assessment (DIRA) for the information system or information handled under this contract as deemed necessary by SSA. A DIRA is required for all public-facing applications and automated telephone services (digital services). The DIRA determines the required identity proofing, authentication, and federation security levels for digital services. Assistance from the Contractor will consist of meeting with the SSA DIRA team and providing all documentation requested, including copies of all screens and a detailed business process description.

a. If the DIRA determination finds that a DIRA is required, the Contractor shall assist SSA with completing documentation required for a DIRA for they system. The Contractor shall provide documentation or information needed to complete this process within a timeframe agreed upon with the COR, but no later than *[insert contract specific timelines]* days after the documentation or information has been requested by the COR.
b. The Contractor shall assist the COR or designee in reviewing the DIRA at least every *[insert contract specific timelines]* throughout the system development lifecycle/information lifecycle, or when the agency determines that a review is required based on a major change to the system, when the system processes new information types, or when the system introduces new or increased digital identity or information security risks, whichever comes first.

14. Rules of Behavior

- Accountability
    - Comply with current information security, privacy, and confidentiality practices.
    - Behave in an ethically, informed, and trustworthy manner.

- Be accountable for all transactions issued in connection with their account credentials.
- Never share password with anyone.
- Have formal authorization from their COR (or other specified management official or representative) before accessing sensitive or critical applications.
- Only use provided access as necessary to execute the contract requirements.

- Integrity
  - Never intentionally enter unauthorized, inaccurate, or false information.
  - Never expose critical data or sensitive information to conditions that may compromise the data's integrity.
  - Review the quality of information as it is collected, or generated to ensure that it is accurate, complete, and up to date.
  - Take appropriate training before using a system.
- Confidentiality
  - Disclose information obtained in the performance of their duties only as necessary to execute the contract requirements and as permitted by agency regulations and guidance and federal regulations, guidance and law.
  - Take precautions to eliminate access or exposure to sensitive information by unauthorized parties or devices.
  - Log-off or lock workstations when leaving devices unattended.
- Awareness and Training
  - Be alert to any indicators of system abuse or misuse.
  - Participate in all required Information Security training and awareness activities as identified by management or required by policy in accordance with EO 13636, 13800, 14028, OMB Circular A-130, and NIST guidance.
    - Complete the mandatory Information Security and Privacy Awareness Training and, if required, Role Based Privacy Training, within agency specified timeframe.
    - Complete role-based information security training to maintain personnel skillsets commensurate with information security job functions necessary for security contract fulfillment, each Fiscal Year for the duration of the contract. The Contractor is responsible for maintaining evidence of completed training and shall provide evidence of such upon SSA request.
- Sensitive Information
  - Protect all sensitive information whether officially on duty or not on duty, at an SSA site, another official work location, or an alternate worksite.

    - Agree to follow all requirements for protecting and handling PII and CUI, including in this contract, FAR and Agency Specific clauses, and any task order issued under this contract.
- Hardware, Software, and Copyright Protection and Control
    - Do not disable any SSA security features unless authorized by management.
    - Use only approved SSA systems resources on SSA equipment. Connecting personally owned hardware, software, and media to SSA systems resources is prohibited.
    - Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices (PED) against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures.
    - Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws.
    - Do not make illegal copies of software.
    - Under no circumstances shall SSA equipment be used for any activity other than official SSA business conducted under this contract and any task order issued under this contract.
    - Comply with all SSA policy and procedures regarding the use of e-mail as well as other forms of electronic communications.
    - Properly safeguard removable media.
- Alternative Worksite (Non-SSA Controlled Locations)
    - Follow the security and safety requirements of an alternative worksite requirements defined in the task order.
    - Adhere to all rules of behavior requirements while at the alternative worksite.
    - Do not print any material that contains PII at non-SSA controlled locations unless specifically allowed in the contract.
    - Safeguard and properly dispose of any other sensitive printed material.
- Public Disclosure
    - Contractor staff that are required to use social media in an official capacity on behalf of the agency must follow the mandatory guidance outlined in this contract and any task order issued under this contract.
    - Ensure the appropriate SSA management officials approve SSA information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers.
    - Never transmit, store, or process sensitive or proprietary SSA information on external sites, unless explicitly authorized to do so. This includes social

media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers.
    - Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.
- Incident Reporting
    - Report suspected virus attacks and malicious/unauthorized intrusion or access in accordance with this contract and any task order issued under this contract.
    - Report suspected violations of the Social Security Act, Privacy Act, and other laws, as well as SSA policies and procedures to the COR.
- **Consequences of Rules Violations**: In those instances where users do not follow the prescribed rules of behavior or violate other agency information security polices, SSA may suspend or remove access to systems or require the return of SSA equipment, any of the above, or other options available under this contract and applicable federal law. SSA may pursue as appropriate other penalties and legal actions. The CO will officially inform the Contractor's representative for the contract of the violation.

15. Physical Location and Data Jurisdiction Requirements

1. The Contractor shall be located, and shall ensure that all federal information is accessed, transferred, stored, or processed, only within the sole jurisdiction of the United States (U.S.) (i.e., any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, American Samoa, Guam, and the Northern Mariana Islands). All Contractor primary locations, back-up facilities or archiving facilities, sites where antivirus and other security scans are performed, and locations of personnel who provide support to SSA in resolving issues regarding the solution, must be physically located within the sole jurisdiction of the United States (as defined). This includes, but is not limited to, the Contractor's primary headquarters facilities, the physical location of all information systems, and the geographical origin of all software used in the execution of this contract.
2. The Contractor shall provide the CO and COR with the specific address for the physical location of all facilities hosting information systems relevant to the execution of this contract. If requested by the CO or COR, the Contractor shall provide physical access to the hosting facility for inspection.

3. At the request of the CO, the Contractor shall provide immediate logical and physical access to all federal information to allow the agency to conduct a review, scan, or a forensic evaluation of any facility where federal information is located. If the federal information is co-located with nonfederal information, the Contractor shall isolate the federal information into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized agency personnel identified by the CO, and without the Contractor's involvement.
4. The Contractor shall notify the CO and COR at least 30 days prior to moving its physical site and within 24 hours when the hosting location of confidential information changes servers or devices. The new location must meet or exceed the security requirements for the current site.

16. Data Protection Requirements

- **Inventory** - The Contractor shall maintain a complete inventory of all hardware and software used in the execution of the contract, including model or version numbers. If the Contractor is processing, storing, or transmitting PII/CUI, the Contractor must indicate in the complete inventory which systems process that information. The Contractor shall provide this inventory information to the CO or COR, upon request.
- **Manufacturer Support** - The Contractor must ensure that all software used in execution of this contract is within one major version of the current version. The Contractor must ensure that all software and hardware used in execution of this contract has manufacturer support. The Contractor must retire or upgrade all software and systems that have reached end-of-life.
- **Standard for Encryption of Electronic Information** - The Contractor shall:
    a) NOT decrypt information they are unauthorized to view.

    b) Encrypt all confidential information (e.g., PII/CUI, proprietary information) in transit (e.g., email, network connections) and at rest (e.g., servers, storage devices, mobile devices, backup media) with FIPS 140-2 (Level 2) validated encryption solution that provides for origin authentication, data integrity, and signer non-repudiation.
    c) Secure all devices (e.g., desktops, laptops, mobile devices) that store and process confidential information and ensure devices meet any SSA specific encryption standard requirements referenced in this contract. Maintain a complete and current inventory of all devices and portable media, as referenced below, that store or process federal information.

d) Verify that it validates the encryption solutions in use under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR upon request.

e) Use the Key Management system on the SSA personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

- **Media Transport** - The Contractor shall:
  a) Document activities associated with the transport of federal information stored on digital and non-digital media.
  b) Digital media, containing federal information that is transported outside of controlled areas shall be encrypted using FIPS 140-2 level 2; non- digital media must be secured using the same policies and procedures as paper.
  c) Media, containing federal information that is transported outside of controlled areas shall be documented in logs, which the agency may request at any time, that include:
     - Identifier and description of what was transported
     - Date of transportation and destination
     - Names of personnel who handled the media during transit outside of controlled areas
     - Date the media was returned or destroyed
     - Name of personnel who received the returned media
     - Notes of any damage to the media at arrival.
- **Boundary Protections -** The Contractor shall ensure that federal information, other than unrestricted information, being transmitted from Federal government entities to external entities is inspected by Trusted Internet Connections (TIC) processes.
- **Configuration Baselines** - The Contractor must ensure that they deploy and operate all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) and software used to process information on behalf of SSA in accordance with approved security configurations and meet the following minimum requirements:
  a) Encrypt equipment and confidential information stored or processed by such equipment in accordance with FIPS 140-2 encryption standards;
  b) Configure all hardware and software in accordance with the latest applicable United States Government Configuration Baseline, Defense Information Systems Agency Security Technical Implementation Guides,

Center for Information Security Benchmarks, or any other minimum security configuration standards as identified by the CO or COR;

c) Maintain the latest operating system patch release and anti-virus software definitions;

d) Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings;

e) Automate configuration settings and configuration management in accordance with SSA security policies, including but not limited to:
   - Configuring its systems to allow for periodic SSA vulnerability and security configuration assessment scanning; and
   - Using Security Content Automation Protocol-validated tools with configuration baseline scanning capabilities to certify all products operate correctly with SSA and NIST defined configurations and do not alter these settings. The Contractor must scan its systems on at least a monthly basis and report the results of these scans to the COR.

- **Federal Websites and Digital Services** - The Contractor must securely configure all new and existing Federal agency public websites and digital services with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain Hypertext Transfer Protocol. For internal-facing websites, the HTTPS is also required.

  Contractors tasked with creating, maintenance, or operating SSA public facing websites must comply with all applicable Federal laws, regulations, and policies, in addition to obtaining agency approval as directed by the COR. SSA public facing websites are subject to federal and agency specific Internet privacy policies and federal security policies including, but not limited to, OMB M-10-22, M-23-22, and any superseding policies.

- **Binding Operational Directives** - The Contractor shall comply with all Binding Operational Directives (BOD). (https://cyber.dhs.gov/directives/)
- **Secure Email Requirements -** The Contractor's corporate or organizational email system is deemed not to be secure. Therefore, the Contractor shall put policies and procedures in place to ensure that its personnel email confidential information using only the following procedures in (a) - (b), below:

a) Sending from an SSA email address. If personnel have been given access to the SSA email system, they must use it to send email messages containing confidential information in the body or in an unencrypted attachment but only to other SSA email addresses (which contain the "name @ssa.gov" format) or to email addresses belonging to an SSA-certified email system. Email directed to any other address(es) may contain confidential information only if the confidential information is entirely contained in an encrypted attachment. The Contractor shall encrypt confidential information in accordance with OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016).
b) Sending from a non-SSA email system. If personnel are using the Contractor's own or any other non-agency email system (e.g., Yahoo!, Gmail), they may send email messages transmitting confidential information only if the confidential information is entirely contained in an encrypted attachment, per OMB Circular A-130; none of the confidential information may be in the body of the email itself or in an unencrypted attachment. When emailing from such systems, this procedure applies when emailing confidential information to any email address, including but not limited to, an SSA email system address. Unless specifically noted otherwise, the Contractor and its employees are expected to conduct business operations under this contract using the Contractor's own email system, i.e., in accordance with the foregoing rules for transmitting confidential information.

Note: SSA may grant written exceptions to compliance with the email requirements above when the Contractor's corporate or organizational email system has been deemed by SSA to be secure.

- **Data Access and Use Requirements** - The Contractor shall:
  a) NOT access, use, or disclose confidential information, except as necessary to execute the contract requirements.
  b) Only disclose confidential information to authorized Contractor personnel who need the information or equipment in the performance of work under this contract. The Contractor shall ensure they establish appropriate administrative, technical, and physical safeguards to ensure that they properly protect security and confidentiality of such information and equipment.
  c) Document all activities associated with the transport of confidential information, including devices and media containing such information, transported outside controlled areas or facilities. This includes the

transport of information stored on digital and non-digital media and mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).

- **Non-Disclosure of Information** - If the Contractor receives a request, subpoena, or court order for agency confidential information, the Contractor will promptly provide (within two business days) the CO notice of such request. The Contractor will provide the agency with the information or tools required for the agency to respond to the request, if necessary. The Contractor shall refer the requester to the agency. The Contractor will not provide a requester any agency confidential information unless authorized by the agency. The Contractor shall not provide testimony in legal proceeding about agency functions or information unless such action is approved by the agency and consistent with 20 C.F.R. Part 403.
- **Data Retention, Inspection, and Disposal Requirements** - The Contractor shall:
    a) Allow the agency the ability to immediately access, search, locate, collect, preserve, amend, and process SSA confidential information as needed to comply with requirements under the provisions of both the Freedom of Information Act (5 U.S.C. § 552); the Privacy Act (5 U.S.C. § 552a); or other Federal law.
    b) Offer capabilities to support the agency's ad hoc legal requirements for E-Discovery, such as litigation preservation obligations, and other preservation or production orders, including meta-data. The Contractor must allow SSA the ability to immediately access, search, locate, collect, preserve, and process SSA confidential information to comply with E-Discovery obligations.
    c) NOT dispose of any SSA information unless authorized by SSA. The Contractor must document and report within 24 hours to the COR all events of accidental disposal or destruction of SSA information without proper authorization as an incident of data loss.
    d) Provide immediate physical and logical access to allow the agency to conduct an inspection. The program of inspection shall include, but is not limited to, conducting authenticated and unauthenticated operating system/network/database/web application vulnerability scans. SSA personnel, or agents acting on behalf of SSA, may perform automated scans. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol standards and the agency approved them. The agency may request the Contractor's scanning results and, at agency discretion, accept those in lieu of agency performed vulnerability scans.

e) At the direction of the COR, within *[Specify Number of Days]* days following the agency's final acceptance of the work under this contract or expiration or termination of this contract, whichever occurs first, the Contractor must return all federal information and IT resources acquired during the term of this contract to the COR, including but not limited to SSA information in non-federal systems, media, and backup systems. The Contractor must provide the agency all materials embodying SSA confidential information (in any form, and including, without limitation, all summaries, copies, excerpts, and metadata of SSA confidential information) to SSA, at no additional cost to SSA. Physical items returned to the agency shall be hand carried or sent by certified mail to the COR.

f) At the direction of the COR, properly sanitize and purge all electronic information obtained in execution of this contract from all Contractor-owned systems including backup systems and media used during contract performance, in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*. The Contractor must provide a certification to the COR that the Contractor properly sanitized, purged, and destroyed electronic and physical records of SSA information obtained in execution of this contract.

- **Audit Record Retention** - The Contractor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to capabilities such as those identified in:
  a) DoD STD-5015.2 V3 (ref. b), Electronic Records Management Software Applications Design Criteria Standard,
  b) NARA Bulletin 2008-05, July 31, 2008, Guidance concerning the use of e-mail archiving applications to store e-mail (ref. c),
  c) NARA Bulletin 2010-05 September 08, 2010, Guidance on Managing Records in Cloud Computing Environments (ref 8).
  d) SSA Information Security Policy (ISP): Low impact systems – at least 30 days; Moderate impact systems – at least 90 days; High impact systems – 7 years.
- **Risk Remediation** - The Contractor shall:
  a) Mitigate security risks for which they are responsible, including those identified during Security Assessment and Authorization (SA&A) and continuous monitoring activities. Remediate all vulnerabilities and other risk findings. As required by the NIST SP 800-53, the Contractor must mitigate high security vulnerabilities and deficiencies identified within agency-defined timelines.
  b) In the event the Contractor cannot mitigate a vulnerability or other risk finding within the prescribed agency timelines, then they must submit to

the COR a Plan of Action & Milestone Report (POA&M) that is approved by the Authorizing Official or designate and mitigate the security vulnerabilities and deficiencies.

- **Security Assessment and Authorization (SA&A)** - The Contractor shall:
    a) Assist SSA with obtaining an SSA Authorization to Operate (ATO) or Security Approval for the proposed solution prior to processing, collecting, or transmitting information. All External Service Providers (ESP) that process or store PII are considered a Moderate impact categorization, at minimum. If PII or sensitive data (defined by the COR) is stored or processed by the ESP, then the ESP shall provide a Security Authorization Package (SAP), which must be reviewed and updated annually to establish and maintain authorization or approval to continue the work. The SAP must include a System Security Plan (SSP), Security Assessment Report (SAR), provided annually by a third-party assessment group, and Plan of Action & Milestone Report (POA&M) with severity and timelines for remediation. All security assessments, reports and resulting POA&Ms must be inline and compliance with all applicable NIST and OMB policies and guidance (NIST 800-37, NIST 800-115, OMB M-02-01, etc.) The ESP shall conduct a triennial reassessment of the information system in which the Contractor shall assess the validity of all current applicable security controls. Additionally, at least annually, the Contractor shall assess a selected subset of the technical, management, and operational security controls employed within the information system. The SAP must be reviewed and approved by SSA before the SSA transfers data to the ESP. Refer to NIST SP 800-37, as updated, for more information on the Security Authorization Package.
    b) SSA's issuance of a signed SSA ATO does not alleviate the Contractor's responsibility to ensure system security and privacy controls are operating effectively on an ongoing basis. The Contractor shall ensure system security and privacy controls are operating effectively on an ongoing basis.
- **Continuous Monitoring** - The Contractor shall maintain a security management continuous monitoring environment that meets or exceeds the requirements of the NIST Risk Management Framework, and the agency information systems continuous monitoring strategy.

17. Access Control Requirements

Multifactor Authentication Multifactor Authentication: The Contractor shall ensure that all IT products and services are:

- Interoperable with SSA issued PIV smart cards
- Compliant with (or authenticate using) approved phishing-resistant Multifactor Authentication mechanism(s), leveraging existing Agency security infrastructure.

The provider shall implement an authentication solution that integrates with SSA's Federation Service to facilitate end user single-sign on using OpenID Connect (OIDC) or SAML (Security Assertion Markup Language) 2.0 standards.

18. Incident Response

The Contractor shall follow the following requirements in the event of an incident involving confidential information. If the Contractor experiences a breach or incident the Contractor shall also follow any additional requirements specific to PII as set forth in the contract.

1. The Contractor shall provide a list of their personnel, identified by name and role, with system administration, monitoring, and/or security responsibilities that are to receive security alerts, advisories, and directives.
2. The Contractor shall have a formal security breach or incident reporting plan approved by the CO or COR. The approved plan shall outline appropriate roles and responsibilities, as well as the steps that must be taken, in the event of a security breach or incident. The plan shall designate who within the Contractor's organization has responsibility for reporting the breach or incident to the agency. The Contractor must follow incident reporting and breach protocols as specified by the agency.
3. The Contractor must cooperate with SSA internal investigation processes with respect to illegal or inappropriate usage of federal information resources including, but not limited to, those investigations conducted by the SSA Chief Human Capital Officer for administrative investigations and those conducted by SSA's Office of the Inspector General.
4. In the event of a suspected or confirmed security-related incident or breach of federal information, the Contractor shall:
    a. Protect all confidential information to avoid a secondary incident with FIPS 140-2 validated encryption.
    b. Limit disclosures about confidential information involved in a breach or incident to only those SSA and Contractor personnel with a need for the information to respond to and take action to prevent, minimize, or remedy the breach or incident. The Contractor may disclose breach or incident information to Federal, state, or local law enforcement agencies and other third parties with a need for the information; however, information about

the specific confidential information involved may only be disclosed to such authorities and third parties as Federal law permits.

c. **NOT**, without SSA approval, publicly disclose information about confidential information involved in a breach or incident or SSA's involvement in a breach or incident.
d. **NOT**, without SSA approval, notify individuals affected by the confidential information breach or incident. The Contractor's confidential information breach and incident reporting process shall ensure that disclosures are made consistent with these requirements.

5. The Contractor shall report all suspected and confirmed security-related incidents and breaches to the SSA COR or designated alternate as soon as possible and without unreasonable delay, **but no later than one (1) hour after discovery**. The Contractor shall provide complete and accurate information about the details of the security-related incident or breach to assist the SSA COR/alternate, including the following information:
    a. Contact information;
    b. A description of the security-related incident or breach (i.e., nature of the incident/breach, scope, number of individuals impacted, type of equipment or media, etc.) including the approximate time and location of the security-related incident or breach;
    c. A description of safeguards used, where applicable (e.g., locked filing cabinet, redacted personal information, password protection, encryption, etc.);
    d. An identification of agency components (organizational divisions or subdivisions) contacted, involved, or affected;
    e. Whether the Contractor has contacted or been contacted by any external organizations (i.e., other agencies, law enforcement, press, etc.); and
    f. Any other pertinent information.
6. The Contractor shall provide full access and cooperate on all activities as determined by the agency to ensure an effective incident and breach response, including providing all requested images, log files, and event information to facilitate rapid resolution of confidential information incidents. This may involve disconnecting the system processing, storing, or transmitting the confidential information from the Internet or other networks or applying additional security controls. This may also involve physical access to Contractor facilities during a breach or incident investigation.

19. Additional Information Security and Privacy Requirements for Cloud-Based Solutions

NOTE: When the Contractor's proposed solution involves or may involve the use of cloud technology, the Contractor must also comply with all the following information security and privacy requirements.

1. **FedRAMP Authorization Requirements** - The Contractor shall comply with FedRAMP SA&A requirements and ensure the information systems and services under this contract have a valid FedRAMP compliant (approved) Authority to Operate (ATO) in accordance with FIPS Publication 199 defined security categorization at the time of contract. If the cloud service product is not listed in the FedRAMP Marketplace (https://marketplace.fedramp.gov/#/products) with a "FedRAMP Authorized" status, the Contractor shall submit a plan to obtain a FedRAMP approved ATO (60) days prior to contract award.
2. **Compliance** - In the event the Cloud Service Provider (CSP) fails to meet both SSA and FedRAMP security and privacy requirements or there is an incident involving confidential information, SSA may suspend or revoke an existing agency ATO (either in part or in whole) and cease operations. If SSA suspends or revokes an agency ATO in accordance with this provision, the CO or COR may direct the CSP to take additional security measures to secure confidential information. These measures may include restricting access to confidential information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the confidential information from the Internet or other networks or applying additional security controls.
3. **SSA Authorization Requirements** - The Contractor shall:
    a. In addition to the FedRAMP compliant ATO, upon SSA's request, complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service. The SSA authorizing official must approve the agency ATO prior to implementation of the system or acquisition of the service.
    b. Identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the Contractor's implementation status as documented in the Security Assessment Report and related continuous monitoring artifacts. In addition, the Contractor shall document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks,

SSA may require remediation at the Contractor's expense, before SSA issues an ATO.

4. **Physical Access Records** - The Contractor shall record all physical access to the cloud storage facilities and all logical access to the federal information as specified in the contract. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the CO or designee in accordance with the contract or upon request to comply with federal authorities.
5. **Availability** - The Contractor shall inform the COR of any interruption in the availability of the cloud service as required by the service level agreement. Whenever there is an interruption in service, the Contractor shall inform the COR of the estimated time that the system or data will be unavailable. The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system and if specified, agreed upon service level agreements (SLA) and system availability requirements. The Contractor must provide regular updates, at intervals specified by the COR, to the COR on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements.
6. **Continued Compatibility** - The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with the agency's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing notification, within 1 hour of discovery, to the COR and shall be responsible for working with the agency to identify appropriate remedies and if applicable, work with the agency to facilitate a smooth and seamless transition to an alternative solution and/or provider.
7. **Service Level Agreement (SLA)** - The Contractor shall understand any applicable terms of the service agreements that define the legal relationships between cloud customers and cloud providers and shall work with SSA to develop and maintain a Service Level Agreement.
8. **Notification Banners** - The Contractor shall display The Standard Mandatory Notice and Consent Banner at log on to all information systems. Choose either banner "a" or "b" based on the character limitations imposed by the system. The formatting of these documents, to include the exact spacing between paragraphs, must be maintained. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."

a. Banner for desktops, laptops, and other devices accommodating banners of 1300 characters.

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

OK

b. For devices with severe character limitations:

I've read & consent to terms in IS user agreem't.

9. **Facility Inspections** - The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by the agency conduct a security audit based on the agency's criteria at least once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with the COR within 20 days of the Contractor's receipt of the audit results. In addition, the agency reserves the right to inspect the facility to conduct its own audit or investigation.
10. **Cloud Security Governance** - The Contractor shall:
    a. Ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act of 2002 (44 U.S.C. § 3551, et seq.), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283)), NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special

Publications 800-53, 800-59, and 800-60. In addition, the Contractor must provide the CO with any documentation it requires for its reporting requirements within 10 days of a request.

b. Make the environment accessible for an agency security team to evaluate the environment prior to the placement of any federal information in the environment and allow for periodic security reviews of the environment during the performance of this contract. The Contractor shall also make appropriate personnel available for interviews and provide all necessary documentation during these reviews.

11. **Maintenance** - The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement to proactively prevent the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, as amended, with special emphasis on assuring that the Contractor's PVM systems and programs apply standardized configurations with automated continuous monitoring to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained to assure all software products deployed in the Contractor's operating environment and serving the agency are compatible with existing systems and architecture of the agency.
12. **Continuous Monitoring** - The Contractor shall provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the COR. In addition, the agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements. If requested, the Contractor will provide the report to the agency within 10 business days.
13. **Penetration Testing** - The SSA reserves the right to perform penetration testing on Contractor's systems, facilities, or cloud services used by the Contractor to deliver services to the SSA. If the agency exercises this right, the Contractor shall allow agency employees (or designated third parties) to conduct security assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning, network device scanning

(to include routers, switches, and firewall), Intrusion Detection System/Intrusion Prevention System, databases, and other applicable systems (including general support structure that support the processing, transportation, storage, or security of SSA confidential information for vulnerabilities).

14. **Risk Remediation** - In the event the Contractor cannot mitigate a vulnerability or other risk finding within the prescribed timelines above, and upon agreement with the CO they shall be added by the Contractor to the designated POA&M and mitigated within the agreed upon timelines. SSA will determine the risk rating of vulnerabilities using FedRAMP baselines.