MASTER MAINTENANCE AGREEMENT (MMA7548)
AMENDMENT 2 AND RENEWAL

This Amendment 2 and Renewal of contract #MMA7548 (the "Renewal") is between the State of Ohio, Department of Administrative Services (the "State") and Great Lakes Computer Corporation (the "Contractor"). This Renewal renews the Master Maintenance Agreement (MMA7548) (the "Contract") for the term set forth below.

WHEREAS, the State and Contractor entered into the Contract on September 5, 2017, expiring on September 30, 2025;

WHEREAS, the State and Contractor desire to renew the Contract; and

WHEREAS, the State and Contractor determined that an amendment is necessary to address certain revisions to the Contract.

NOW, THEREFORE, the Contract is amended and renewed as follows:

1. Pursuant to Section 1 of the Contract, the term of the Contract is renewed for an additional term of two years, beginning on October 1, 2025 and ending on September 30, 2027.

2. Delete Section 6, Contractor Quarterly Sales Report, in its entirety and replace it with the following:

   6. QUARTERLY REPORTING

   The Contractor must report the quarterly dollar value (in U.S. dollars and rounded to the nearest whole dollar) of the sales to Cooperative Purchasing Members under this Contract each calendar quarter (i.e., January-March, April-June, July-September, and October-December). The dollar value of the sales reported must equal the price paid by all Cooperative Purchasing Members for purchases under this Contract during the reporting period. The sales to State agencies under this Contract are automatically reported in OhioBuys.

   The Contractor must submit the quarterly sales reports to the State via OhioBuys. If no sales occur, the Contractor must still submit the quarterly sales report and show zero sales for the quarter on the report. The reports must be submitted no later than 30 days after the completion of the reporting period.

   The Contractor must also submit a closeout report within 120 days after the expiration of this Contract. For purposes of this provision, the Contract expires on the physical completion of the last outstanding task or order of the Contract. The close-out report must cover all sales not shown in the final quarterly report and reconcile all errors and credits. If the Contractor reported all Contract sales and reconciled all errors and credits on the final quarterly sales report, then the closeout report should show zero sales.

   If the Contractor fails to submit any sales report in a timely manner or falsifies any sales report, the State may terminate this Contract for cause.

3. Delete Section 7, Contractor Revenue Share, in its entirety and replace it with the following:

   7. REVENUE SHARE

   The Contractor must pay to the State a share of the sales transacted under this Contract as a fee to the State to cover the estimated costs the State will incur in administering this Contract and the Services offered under it ("Revenue Share").

   The Contractor must remit the Revenue Share in U.S. dollars within 30 days after the end of the quarterly reporting period. The Revenue Share that the Contractor must pay under this Contract equals ¾ of 1% of the total quarterly sales reported. The Revenue Share must be

included in the prices reflected in any order and reflected in the total amount charged to the State, and the Contractor may not add a surcharge to orders under this Contract to cover the cost of the Revenue Share.

The Contractor must remit any amount due as the result of a quarterly or closeout sales report at the time the quarterly or closeout sales report is submitted to the Department of Administrative Services, Office of State Purchasing. To ensure the payment is credited properly, the Contractor must identify the payment as a "State of Ohio Revenue Share" and include this Contract number, total report amount, and reporting period covered.

Contractor will pay the Revenue Share by check remittance, both normal and overnight, credit card payment via the State's epayment portal, or ACH payment, if approved by the State, using the instructions below.

Check remittance: Follow the remittance instructions on the required Quarterly Sales Report and Revenue Share Remittance Form at the following link, https://das.ohio.gov/revenueshareform.

Credit Card Payments: To pay by credit card, use the following link, https://epay.das.ohio.gov/Payment, select "Revenue Share" as the payment type and follow the on-screen prompts.

ACH Payments: If this payment method is approved by the State, the State will provide payment instructions to Contractor.

If the full amount of the Revenue Share is not paid within 30 days after the end of the applicable reporting period, the non-payment will constitute a contract debt to the State. The State may setoff any unpaid Revenue Share from any amount owed to the Contractor under this Contract and employ all other remedies available to it under Ohio law for the non-payment of the Revenue Share. Additionally, if the Contractor fails to pay the Revenue Share in a timely manner, the failure will be a breach of this Contract, and the State may terminate this Contract for cause as set forth herein and seek damages for the breach.

4. Delete Section 29, Equal Employment Opportunity, in its entirety and replace it with "**RESERVED**."

5. Delete Section 30, Drug Free Workplace, in its entirety and replace it with the following:

30. DRUG FREE WORKPLACE

The Contractor agrees to comply with all applicable state and federal laws regarding drug-free workplace and must make a good faith effort to ensure that all Contractor employees, while working on State property or performing work on behalf of the State, will not purchase, transfer, use, be under the influence of, or possess illegal drugs, non-medical cannabis (recreational marijuana), or alcohol, or abuse prescription drugs or medical marijuana in any way.

6. Delete Section 39, Prohibition of the Expenditure of Public Funds for Offshore Services, in its entirety and replace it with the following:

39. PROHIBITION OF THE EXPENDITURE OF PUBLIC FUNDS FOR OFFSHORE SERVICES

No State Cabinet Agency, Board or Commission will enter into any contract to purchase services provided outside of the United States or that allows State Data to be sent, taken, accessed, tested, maintained, backed up, stored, or made available outside of the United States, unless the Contracting Agency obtains a duly signed waiver from the State. Notwithstanding any other terms of this Contract, the State reserves the right to recover any funds paid for services the Contractor performs or for data located outside of the United States for which a waiver was not received. The State does not waive any other rights and remedies

provided to the State in this Contract.

Further, no State agency, board, commission, State educational institution, or pension fund will make any purchase from or investment in any Russian institution or company. Notwithstanding any other terms of this Contract, the State reserves the right to recover any funds paid to Contractor for purchases or investments in a Russian institution or company in violation of this paragraph.

The Contractor must complete the Contractor/Subcontractor Affirmation and Disclosure Form affirming the Contractor understands and will meet the requirements of the above prohibition. During the performance of this Contract, if the Contractor changes the location(s) disclosed on the Affirmation and Disclosure Form, Contractor must complete and submit a revised Affirmation and Disclosure Form to the Contracting Agency reflecting such changes. The applicable provisions of this section will expire if the applicable Executive Order is no longer effective.

7. Delete Section 41, Independent Contractor Acknowledgement, in its entirety and replace it with the following:

41. INDEPENDENT CONTRACTOR ACKNOWLEDGEMENT

It is fully understood and agreed that Contractor is an independent contractor and is not an agent, servant, or employee of the State. Contractor declares that it is engaged as an independent business and has complied with all applicable federal, state, and local laws regarding business permits and licenses of any kind, including, but not limited to, any insurance coverage, workers' compensation, or unemployment compensation that is required in the normal course of business and will assume all responsibility for any federal, state, municipal or other tax liabilities. Additionally, Contractor understands that as an independent contractor, it is not a public employee and is not entitled to contributions from the State to any public employee retirement system.

Contractor acknowledges and agrees that any individual providing personal services under this Contract is not a public employee for purposes of Chapter 145 of the Ohio Revised Code. Unless Contractor is a "business entity" as that term is defined in Section 145.037 of the Ohio Revised Code ("an entity with five or more employees that is a corporation, association, firm, limited liability company, partnership, sole proprietorship, or other entity engaged in business"), Contractor must have any individual performing services under the Contract complete and submit to the Ordering Agency the Independent Contractor/Worker Acknowledgement form.

Contractor's failure to complete and submit the Independent Contractor/Worker Acknowledgement form at the time Contractor executes this Contract will serve as Contractor's certification that Contractor is a "business entity" as that term is defined in Section 145.037 of the Ohio Revised Code.

8. Delete Section 42, Boycotting in its entirety and replace it with the following:

42. TRADE

Pursuant to Section 9.76(B) of the Ohio Revised Code, Contractor warrants that Contractor is not boycotting any jurisdiction with whom the State of Ohio can enjoy open trade, including Israel, and will not do so during the Contract period.

The State of Ohio does not acquire supplies or services that cannot be imported lawfully into the United States or transact business with any entity or individual subject to financial sanctions imposed by the United States. The Contractor certifies that it, its subcontractors, and any agent of the Contractor or its subcontractors, will acquire any supplies or services in

accordance with all trade control laws, regulations or orders of the United States, including the prohibited source regulations set forth in subpart 25.7, Prohibited Sources, of the Federal Acquisition Regulation and any sanctions administered or enforced by the U.S. Department of Treasury's Office of Foreign Assets Control. A list of those entities and individuals subject to sanctions can be found at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-andblocked-persons-list-sdn-human-readable-lists. These sanctions generally preclude most transactions involving Cuba, Iran, and Sudan, and most imports from Burma or North Korea.

9. In the Contract, add the following new Section 43, OhioBuys:

43. OHIOBUYS

OhioBuys is an electronic procurement system that provides electronic contract and catalog hosting and management services. Ordering Agencies access this system to place orders for the procurement of goods and services using State of Ohio contracts. The Contractor agrees to establish, maintain and support its contract and catalog, if applicable, in OhioBuys.

10. In the Contract, add the following new sections:

44. DATA SECURITY AND PRIVACY TERMS

The Contractor must comply with the Data Security and Privacy Terms attached to this Contract as Exhibit 1 and incorporated as if fully rewritten herein.

45. AMENDMENTS – WAIVER

Amendments. No change to any provision of this Contract will be effective unless it is in writing and signed by the parties to the Contract. Unless specifically provided otherwise in this Contract or agreed to in writing by the Contracting or Ordering Agency, no terms or conditions included on a Contractor's quote or ordering document will be valid or enforceable against the State and are specifically excluded from this Contract. Further, no "click-through," "shrink-wrap," "browse-wrap," or other terms that have not been specifically negotiated by the Contractor and the State, whether before, on, or after the date of this Contract, will be effective to add or modify the terms of this Contract, regardless of any party's "acceptance" of those terms by electronic means.

Waiver. The failure of either party at any time to demand strict performance by the other party of any of the terms of this Contract will not be a waiver of those terms or to any other terms of this Contract. Waivers must be in writing to be effective, and either party may at any later time demand strict performance.

46. LEGAL REPRESENTATION AND RIGHTS

The Ohio Attorney General is the chief law officer for the State of Ohio, its agencies, boards and commissions, and only the Ohio Attorney General has the authority to appoint outside legal counsel to represent the State. Contractor agrees that any provisions in this Contract or any documents incorporated by reference that provide or allow for outside legal representation to defend or settle claims on behalf of the State or provide for a third party to have sole control of a defense or settlement of a claim do not meet the requirements of state law and are considered stricken. Contractor also agrees that, unless specifically agreed to in writing by the State, any provisions that require or provide for a waiver of any legal rights, remedies, or litigation defenses (i.e., waiver of a jury trial) do not meet the requirements of state law and are considered stricken.

47. STATUTE OF LIMITATIONS

Statutes of limitations generally do not apply to actions brought by the State and any such provisions in this Contract or in any documents incorporated by reference are considered stricken.

48. ACCESSIBILITY REQUIREMENTS

If applicable, the Contractor warrants it will comply with federal and state disabilities laws and regulations and also warrants that the products and services provided under this Contract conform to the applicable accessibility requirements of WCAG 2.1 Level AA or the most current version (the "Accessibility Standards"), Section 508 of the Rehabilitation Act of 1973, and the Americans with Disabilities Act. The Contractor must promptly respond to and resolve any complaint regarding accessibility of its products and services. If at any time, the products and services provided under this Contract do not fully conform to the Accessibility Standards, the Contractor must immediately notify the State in writing of the nonconformance and provide to the State a plan to achieve conformance to the Accessibility Standards, including an intended timeline for conformance. The Contractor further agrees to indemnify and hold harmless the State from any claims or damages arising out of Contractor's failure to comply with the requirements of this section. Failure to comply with these requirements shall constitute a material breach of this Contract for which the State may terminate this Contract.

11. Delete the Standard Affirmation and Disclosure Form, Executive Order 2011-12K attachment in its entirety.

12. Add Exhibit 1, Data Security and Privacy Terms, attached to this Amendment to the Contract.

This Renewal shall become effective as of the date of the State's signature and shall remain in full force and effect for the term of the Agreement. Except as modified by this Renewal, all other terms, conditions and pricing of the Agreement shall remain the same and in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Renewal as of the dates appearing below.

GREAT LAKES COMPUTER CORPORATION	**STATE OF OHIO DEPARTMENT OF ADMINISTRATIVE SERVICES**
By:	**By:** E-SIGNED by Kathleen C. Madden /rlg on 2025-08-26 17:14:48 GMT
Name: Robert Martin	**Name:** Kathleen C. Madden
Title: PRESIDENT	**Title:** Director
Date: 8/14/2025	**Date:**

EXHIBIT 1
DATA SECURITY AND PRIVACY TERMS

These Data Security and Privacy Terms ("Terms") describe the responsibilities for the Contractor relating to State information security and privacy standards and requirements for all proposed solutions, whether cloud, on-premises, or hybrid based. These Terms apply to all work, services, and personnel across all environments, and State of Ohio ("State") and Contractor locations (e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid) along with the computing elements that the Contractor will perform, provide, occupy, or utilize in performing the work, and any Contractor access to State resources in conjunction with the delivery of work.

The Contractor must comply with these Terms as they apply to the services being provided to the State. The Contractor is responsible for maintaining information security in any environments under the Contractor's management in accordance with these Terms.

These Terms are in addition to the Contract terms and conditions. In the event of a conflict between the Contract and these Terms, the most stringent standard will prevail.

Definitions

1. **Contract** means the contract entered into between the Contractor and the State to which these Terms are attached and/or incorporated.

2. **Contract Data** means State Data that the Contractor has access to, transmits, processes, possesses, creates or stores in providing services to the State.

3. **Contractor** means the person or entity with whom the State has entered into the Contract and, for purposes of these Terms, includes subcontractors or other personnel under the authority or control of the Contractor performing the work or providing the services under this Contract.

4. **Personally Identifiable Information** as defined in the Ohio Revised Code means information that can be used directly or in combination with other information to identify a particular individual. It includes:
   A. A name, identifying number, symbol, or other identifier assigned to a person,
   B. Any information that describes anything about a person,
   C. Any information that indicates actions done by or to a person,
   D. Any information that indicates that a person possesses certain personal characteristics.

5. **Security Event** is any observable occurrence that is relevant to information security within normal operational noise levels and below pre-defined incident thresholds that does not adversely impact or potentially impact Contract Data or information systems.

6. **Security Incident** means there is successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

7. **State Data** means all data and information provided by, created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Confidential Data. All State Data is and will remain the property of the State and, unless specifically provided otherwise in the Contract, Contractor acquires no right, title, or interest in or to State Data.

8. **Confidential Data** means any type of data that is required to be protected by law or regulation, is intended for confidential use, and may not be copied or removed from the State's operational control without authorized permission. Confidential Data includes data that, if compromised, may result in loss of life, serious injury, or other harm to an individual or group, or disruption to critical State operations. Confidential Data is included in the definition of Confidential Information in the Contract.

Confidential Data includes, but is not limited to:

A. Personally Identifiable Information (PII);
B. Student information under the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g);
C. Federal Tax Information (FTI) under IRS Publication 1075 - Tax Information Security Guidelines for federal, state, and local agencies;
D. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164); United States Code 42 U.S.C. 1320d through 1320d-9 (HIPAA); and Code of Federal Regulations for Public Health and Public Welfare: 42 C.F.R. 431.300, 431.302, 431.305, 431.306, 435.945, 45 C.F.R. 164.502(e) and 164.504(e);
E. Criminal Justice Information (CJI) under the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy available at https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center;
F. Payment Card Industry Data Security Standards (PCI DSS);
G. Social Security Administration (SSA) Data which is data received by the State from the Social Security Administration in accordance with the current Computer Matching and Privacy Protection Act between the State of Ohio and the Social Security Administration; and
H. Other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.

9. **State IT Security Policies and Standards** means the policies and standards available at https://das.ohio.gov/technology-and-strategy/information-security-privacy/information-security-governance.

Requirements

1. The Contractor's Responsibilities Generally

At a minimum, the Contractor must maintain the security of Contract Data in accordance with the moderate level security baseline of the current published version of the National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," (NIST 800-53). In the alternative, the Contractor may maintain the security of Contract Data in accordance with International Organization for Standardization 27001 (ISO 27001) if the Contractor implements the additional necessary controls to achieve compliance with the requirements of NIST 800-53. Hereinafter, references in these Terms to "NIST 800-53" means both of the frameworks defined in this paragraph.

The Contractor must implement the information security policies, standards, and capabilities set forth in the Contract, support the State's adherence to the State IT Security Policies and Standards, and use procedures in a manner that does not diminish established State capabilities and standards.

If the Contractor accesses the State's facilities or networks, or provides products, solutions, or services that will be implemented or integrated in the State's controlled environment, the Contractor must ensure its products, solutions, or services comply with State IT Security Polices and Standards, as appropriate (available at the link provided above in the definition of State IT Security Policies and Standards).

The Contractor's information security and technology responsibilities with respect to the work and services the Contractor is providing to the State include the following, where applicable:

A. Assist in the implementation of associated security procedures with the State's review and approval, including physical access requirements, User ID approval procedures, and a Security Incident action and response plan.

B. Support implementation and compliance monitoring as per the State IT Security Policies and Standards.

C. Upon identification of a potential issue with maintaining an "as provided" State infrastructure element in accordance with a more stringent State level security policy, the Contractor must identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies for consideration by the State.

2. Protection and Handling of Contract Data

The Contractor must maintain an information security program made up of policies, procedures, technical and organizational safeguards, and training designed to protect Contract Data against unauthorized loss, destruction, alteration, access, or disclosure. To protect Contract Data, the Contractor must use due diligence to ensure that computer and telecommunications systems and services involved in storing, using, or transmitting Contract Data are secure and prevent Contract Data from unauthorized disclosure, modification, use, or destruction. To accomplish this, the Contractor must adhere to the following requirements regarding Contract Data in addition to the confidentiality requirements in the Contract:

A. Assume all Contract Data is both confidential and critical for State operations.

B. Maintain, in confidence, Contract Data it may obtain, maintain, process, or otherwise receive from or through the State during the term of the Contract and pursuant to the provisions of the Contract and these Terms.

C. Use and permit its employees, officers, agents, and subcontractors to use any Contract Data received from the State solely to perform its obligations under the Contract.

D. Not sell, rent, lease, disclose, or permit its employees, officers, agents, and subcontractors to sell, rent, lease, or disclose, any Contract Data to any third party, except as permitted under the Contract or required by applicable law, regulation, or court order.

E. Take all commercially reasonable steps to (a) protect the confidentiality of Contract Data received from the State and (b) establish and maintain physical, technical, and administrative safeguards to prevent unauthorized access by third parties to Contract Data received by the Contractor from the State.

F. Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of Contract Data.

G. Ensure that the Contractor's internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability of Contract Data, and periodically review and update these policies, plans, and procedures as needed.

All Contract Data at rest in systems supporting the Contractor's services must reside within the contiguous United States with a minimum of two data center facilities at two different and distant geographic locations, ensuring physical and environmental protection controls are implemented as defined in State IT Security Policy 2100-15, and be handled in accordance with the requirements of these Terms at all Contractor locations. All Contract Data that is not classified as public by the State must be encrypted at rest and while in transit utilizing industry standards that meet Federal Information Processing Standards (FIPS) validated algorithms and comply with State IT Security Policy IT-14, Securing Confidential Data.

If the Contractor will be accessing, processing, transmitting, possessing, creating, or storing Confidential Data, the State may require additional documentation from the Contractor and/or input to complete State documentation.

3. Security Standards and Warranties

All solutions shall operate at the moderate level baseline as defined in the current published version of NIST 800-53, be consistent with Federal Information Security Management Act, 44 U.S.C. § 3551 et seq.

(FISMA 2014) requirements and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications.

The Contractor's information security program must be designed to protect Contract Data by implementing an industry security and privacy standard including, at a minimum:

A. Security and confidentiality of Contract Data.

B. Protection against anticipated threats or hazards to the security or integrity of Contract Data.

C. Protection against unauthorized access to, disclosure of, or use of Contract Data.

D. Giving access to Contract Data only to those individual employees, officers, agents, and subcontractors who need to know such information in connection with the performance of the obligations under the Contract.

E. Cooperating with any attempt by the State to monitor compliance with the foregoing obligations as reasonably requested by the State.

F. Promptly destroying or returning to the State, in a format designated by the State, all Contract Data received from or through the State upon completion of the work under the Contract or upon termination or expiration of the Contract. Notwithstanding the foregoing, the Contractor may keep a copy of the Contract Data to comply with contractual, legal, or record keeping obligations, and any such retained Contract Data is subject to the requirements of this Contract for so long as the Contractor has the Contract Data in its possession.

G. Maintaining appropriate and effective business continuity and disaster recovery plans to ensure resiliency of Contract Data and business operations.

H. Maintain a privacy policy that includes, at a minimum, processes for the State to obtain individual privacy consent for the use of PII, at the determination of the State, and to respond to individuals' requests to access, correct, and delete their PII unless otherwise expressly agreed to in the Contract. All PII, including PII that has been de-identified, is considered Contract Data and Confidential Information under this Contract.

The Contractor must scan all source code for vulnerabilities, including before and after any source code changes are made, must promptly remediate vulnerabilities, and/or provide the State with patches to address the vulnerabilities at no cost to the State. The Contractor must follow best practices for application code review and the most current version of the Open Source Foundation for Application Security (OWASP) top 10.

In addition to the warranties provided and pursuant to the terms of the warranties section of the Contract (i.e., notification, correction, and indemnification), the Contractor warrants that its software is free from viruses, malware, and other harmful or malicious code.

4. Permitted Disclosure to Third Parties

Disclosure of Contract Data is permitted as set forth in the Contract. Additionally, disclosure of Contract Data is also permitted when required by applicable law, regulation, court order, or subpoena. If the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether Confidential Data or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process or otherwise believes that disclosure is required by any law, ordinance, rule or regulation, the Contractor must notify the State within 24 hours of receipt of the order or request in order for the State to seek a protective order or take other appropriate action, as desired. The Contractor must also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State.

If, in the absence of a protective order, the Contractor is compelled as a matter of law to disclose the information provided by the State, the Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, the Contractor must advise and consult with the State and its counsel as to the scope of such disclosure and the nature of wording of such disclosure) and must use commercially reasonable efforts to obtain confidential treatment for the information disclosed.

The Contractor may disclose Confidential Information to the following people, subject to the requirements of the Contract and these Terms:

A. To State or Federal auditors or regulators.

B. To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations.

C. To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

5. Auditing

A. If the Contractor provides a solution, service, or product hosted by the Contractor or a cloud provider, the Contractor must obtain an annual audit of the services being provided under this Contract that meets the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements (SSAE) No. 18, Service Organization Control 2 Type 2 (SOC 2 Type 2). At any point during the term of the Contract and if not already obtained, the Contractor may obtain and must thereafter maintain StateRAMP or FedRAMP authorization in lieu of a SOC 2 Type 2 audit.

B. If Contractor provides a solution, service, or product hosted by the Contractor or a cloud provider that completes a financial duty on behalf of the State, the Contractor must obtain an annual audit of the services being provided under this Contract that meets the AICPA SSAE No. 18, Service Organization Control 1 Type 2 (SOC 1 Type 2).

C. The SOC 1 Type 2 and SOC 2 Type 2 audits will be completed at the sole expense of the Contractor and the results must be provided to the State within 30 days of the Contractor's receipt of its audit results each year by emailing the results to Compliance@das.ohio.gov. The results of the audits provided to the State are considered Confidential Information under the Contract.

D. When required by law, rule, or regulation, or if the Contractor does not obtain or obtains an adverse opinion on the SOC 2 Type 2 audit described above, the State may, at any time in its sole discretion, elect to perform a security and data protection audit. This includes a thorough review of Contractor controls, security and privacy functions and procedures, data storage and encryption methods, and backup and restoration processes. The State may utilize a third-party contractor to perform such activities to demonstrate that all security, privacy, and encryption requirements are met. The State will provide its request in writing and will work with the Contractor to schedule time to conduct the audit.

E. At no cost to the State, the Contractor must remedy material issues, material weaknesses, or other items identified in each audit as they pertain to the services provided under this Contract.

6. Background Investigations of Contractor Personnel

Any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a

Specially Designated National, or (c) has been convicted of a felony may not perform certain services under the Contract.

The Contractor must conduct background investigations on Contractor personnel that may have access to Contract Data. The State may conduct background investigations on Contractor personnel that have or may have access to Confidential Data, critical infrastructure systems, or when required by law, rule, or regulation. The State will conduct initial background investigations on Contractor personnel who will have access to FTI and/or CJI that must be favorably adjudicated before being permitted to access the FTI and/or CJI, and ongoing background investigations every five years thereafter for personnel who already have access to FTI and/or CJI.

If any Contractor personnel refuses to have a background investigation completed or has an unfavorably adjudicated background investigation completed, the State may terminate that personnel's access to the Contract Data.

7. Security Incidents and Events

A. Categories

Security Incidents may fall into one or more of, but are not limited to, the following categories:

i. Loss or Theft
ii. Denial of Service (DoS)
iii. Improper Usage or Access
iv. Information Spillage
v. Malicious Code
vi. Phishing Messages
vii. Scans/Probes/Attempted Access
viii. Social Engineering
ix. Unauthorized Access

Security Events may fall into one or more of, but are not limited to, the following categories:

i. Unsuccessful log-on attempts
ii. Unsuccessful denial of service attacks
iii. Unsuccessful phishing attacks
iv. Unsuccessful network attacks such as pings, probes of firewalls, or port scans.

B. Security Incident Response and Reporting

The Contractor is responsible for Security Incident response, including containment, eradication, and recovery, to minimize the impact to the State. In addition to the requirements in the Contract, the Contractor must perform the following in response to a Security Incident involving Contract Data.

The Contractor is not required to report Security Events unless a pattern of attacks significantly increases the risk of impact.

The Contractor must report in writing to the State within 24 hours of the Contractor becoming aware of any Security Incident and/or use or disclosure of Contract Data not authorized by the Contract, including any reasonable belief that unauthorized access to or acquisition of Contract Data has occurred, and fully cooperate with the State to mitigate the consequences of the Security Incident. Within five business days of the initial Security Incident report to the State, the Contractor must document and begin providing follow-up reports for all Security Incidents to the State. The Contractor must provide updates to the follow-up reports until the investigation is complete. At a minimum, the Security Incident reports will include:

i. Data elements involved, the extent of the Contract Data involved in the Security Incident, and the identification of affected individuals, if applicable.

ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed Contract Data, or to have been responsible for the Security Incident.

iii. A description of where the Contract Data is believed to have been improperly transmitted, sent, or utilized, if applicable.

iv. A description of the probable causes of the Security Incident and, in the final report, the root cause.

v. A description of the proposed plan for preventing similar future Security Incidents, including a recommended risk remediation plan.

vi. A description of the corrective actions taken, including repair (elimination of a defect or incident and/or restoration of system functionality requirements according to the Contract) and resolution (a temporary workaround to enable system function).

vii. Whether the Contractor believes any federal or state laws requiring notifications to individuals are triggered.

The Contractor must comply with all applicable laws that require the notification of individuals, or with other reasonable direction of the State for notification, in the event of a Security Incident involving personally identifiable information, or any other event requiring such notification. The State may, in its sole discretion, choose to provide notice to any or all parties affected by a Security Incident, but the Contractor shall reimburse the State for the cost of providing such notification. Contractor further agrees to provide, or to reimburse the State for its costs in providing, any credit monitoring or similar services that are necessary as a result of Contractor's Security Incident. Under Ohio law, Contract Data is State property and any illegal activity involving State property is subject to a criminal investigation. The Contractor shall preserve sufficient evidence to ensure accurate Security Incident records, facilitate an investigation, and determine the extent of the Security Incident.

The Contractor shall work with the State to establish a Security Incident reporting communications procedure including Contractor and State contacts, communication methods and tools. If there is no procedure established, the Contractor must report Security Incidents to the primary contact listed in the Contract or that contact's successor and the Contractor must report the Security Incident to the State via email at CSC@ohio.gov or call 877.644.6860.

The State reserves the right to conduct an independent investigation of the Security Incident, and the Contractor shall cooperate with the investigation. The independent investigation may be conducted by a State agency or a third party acting on behalf of the State.

8. Generative Artificial Intelligence

The Contractor must disclose the use of generative artificial intelligence (AI) to the State when producing work that will be owned by the State or the integration of generative AI in products or services used by the State. The Contractor must work with the State to ensure the use of generative AI is reviewed, approved, and complies with the State IT Policy IT-17, Use of Artificial Intelligence, prior to utilizing the generative AI components. The Contractor is not permitted to utilize Confidential Data in training generative AI models except as specifically approved by the State.

9. Contractor Access

When the Contractor accesses State network systems, data, and facilities, including remotely, the Contractor must maintain a robust security capability that incorporates generally recognized system hardening techniques. The Contractor must use appropriate measures to ensure that Contract Data is secure before transferring control of any systems or media on which Contract Data is stored. The method of securing the Contract Data must be in alignment with the required data classification. The Contractor may permit Contract Data to be loaded onto portable computing devices or portable storage components or media only if adequate security measures are in place to ensure the integrity and security of Contract Data and the Contract Data is encrypted. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under the Contract. The Contractor shall use multifactor authentication to limit access to systems that contain Confidential Data.

The Contractor must also maintain an accurate inventory of all such devices and the individuals to whom they are assigned. The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with Contract Data and must report any loss or theft of such devices containing Contract Data to the State in writing as defined in Section 7.

10. Family Educational Rights and Privacy Act

When the Contractor is handling Contract Data that includes student information, the Contractor must comply with all applicable provisions of Ohio and federal laws regarding student information, including Parts B and C of the Individuals with Disabilities Education Act (20 U.S.C. 1400 and Title 34 of the Code of Federal Regulations Part 300, and 20 U.S.C. 1400 and Title 34 of the Code of Federal Regulations Part 303, respectively) and the Family Educational Rights and Privacy Act (20 U.S.C. 1232) (FERPA) or its State equivalent including any amendments or other relevant provisions of federal law as well as all requirements of Chapter 99 of Title 34 of the Code of Federal Regulations. Nothing in this Contract shall be construed to allow either party to maintain, use, disclose, or share student information in a manner not allowed by either state or federal laws or regulations.

11. HIPAA Compliance

When the Contractor is handling Contract Data that includes health or medical data, the Contractor must comply with the data handling and privacy requirements of HIPAA and its associated regulations. Additionally, some or all of the Contract Data may be client identifying information covered by 42 C.F.R. Part 2. Contractor may only disclose such client identifying information back to the State and is bound in all respects by the regulations of 42 C.F.R. Part 2. If required, the Contractor must execute a business associate agreement with the State when handling protected health information.

12. Federal Tax Information

When the Contractor is handling Contract Data that includes Federal Tax Information (FTI), the Contractor must comply with the IRS Publication 1075 safeguards below.

All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements defined in Internal Revenue Service (IRS) Publication 1075. The language in this Section may not be modified by Contractor and any proposed language changes listed in Contractor's responses in this section will not be considered. For purposes of this section, "agency" means the applicable State entity.

A. Performance

In the performance of the Contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

i. All work will be performed under the supervision of the contractor.

ii. The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.

iii. FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

iv. FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.

v. The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

vi. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

vii. All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

viii. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.

ix. Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.

x. To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

xi. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract.

xii. For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

xiii. The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

B. IRS 1075 Criminal/Civil Sanctions

i. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

ii. Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

iii. Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

iv. Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

v. Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, *Sanctions for Unauthorized Disclosure*, and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

C. Inspection

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

13. Criminal Justice Information

When the Contractor is handling Contract Data that includes criminal justice information (CJI), the Contractor must comply with the requirements in this section.

Contractor acknowledges that this Contract is subject to the requirements, conditions and restrictions set forth in: (i) the National Crime Information Center (NCIC) Operating Manual (available at http://www.cjis.gov, call the help desk); (ii) the Criminal Justice Information Services (CJIS) Security Policy (available at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view); and (iii) Title 28, Code of Federal Regulations, Part 20 (available at http://www.gpo.gov/fdsys/pkg/CFR-2010-title28-vol1/pdf/CFR-2010-title28-vol1-part20.pdf) as the manual, policy, and regulations may be revised, amended or replaced. Further, Contractor shall require all employees, independent contractors and/or any other consultant performing work for the Contractor under this Contract to complete and submit to the State the Certification page of the Federal Bureau of Investigation, CJIS Security Addendum and Certification set forth in Appendix H of the CJIS Security Policy, the relevant portions of the current version are attached to these Terms below.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.
>
> The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and

personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

§ 20.33 Dissemination of criminal history record information.

a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:

1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.

2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and

3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government tprivate sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Debbie Tsiros / Debbie Tsiros — 8/14/2025
Printed Name/Signature of Contractor Employee — Date

Robert Martin — 8/14/2025
Printed Name/Signature of Contractor Representative — Date

GREAT LAKES Computer Corp. / President
Organization and Title of Contractor Representative

SUMMARY OF AMENDMENTS

Amendment Number	Effective Date	Description
2	Pending	Renew contract and update terms and conditions.
1	9/9/2019	Renew contract and update terms and conditions.