

Contract Abstract

Contract Information

Contract & Solicitation Title:

Contract Summary:

Contract Number: Solicitation Number: Requisition Number:

Replaces Expiring or Expired Contract? (Enter "No" or Contract No and Expiration Date):

Type of Contract/PO: **Requires Council Legislation:** **Yes**

High Risk Contract (Per Finance Department Contract Risk Management Policy): **No**

Sexual Harassment Training Required (per BL2018-1281): **Yes**

Estimated Start Date: Estimated Expiration Date: Contract Term:

Estimated Contract Life Value: Fund:* BU:*

(*Depending on contract terms, actual expenses may hit across various departmental BUs and Funds at PO Levels)

Payment Terms: Selection Method:

Procurement Staff: BAO Staff:

Procuring Department: Department(s) Served:

Prime Contractor Information

Prime Contracting Firm: ISN#:

Address: City: State: Zip:

Prime Contractor is a : SBE SDV MBE WBE LGBTBE (select/check if applicable)

Prime Company Contact: Email Address: Phone #:

Prime Contractor Signatory: **Email Address:**

Business Participation for Entire Contract

Small Business and Service Disabled Veteran Business Program:

Amount: Percent, if applicable:

Equal Business Opportunity (EBO) Program:

MBE Amount: MBE Percent, if applicable:

WBE Amount: WBE Percent, if applicable:

Federal Disadvantaged Business Enterprise:

Amount: Percent, if applicable:

Note: Amounts and/or percentages are not exclusive.

B2GNow (Contract Compliance Monitoring):

Summary of Offer

Offeror Name	MBE	WBE	SBE	SDV	LGBTBE	Score	Evaluated Cost	Result
	(check as applicable)					(RFP Only)		
<input type="text" value="NEC Corporation of America"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="N/A"/>	<input type="text" value="N/A"/>	<input type="text" value="Approved Sole Source Form"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Select from the Following:"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Select from the Following:"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Select from the Following:"/>



Terms and Conditions

1. GOODS AND SERVICES CONTRACT

1.1. Heading

This contract is initiated by and between **The Metropolitan Government of Nashville and Davidson County (METRO)** and **NEC Corporation of America (CONTRACTOR)** located at **3929 W. John Carpenter Frwy, Irving, TX 75063**, resulting from an approved sole source signed by Metro's Purchasing Agent (made a part of this contract by reference). This Contract consists of the following documents:

- *Any properly executed contract amendment (most recent with first priority),*
- *This Contract,*
- *Exhibit A - MISA Terms and Conditions*
- *Exhibit B - Scope of Work, including Pricing*
- *Exhibit C - Biometric Master Purchase and Sale Agreement*
- *Exhibit D - Affidavits*
- *Purchase Orders (and PO Changes)*

In the event of conflicting provisions, all documents shall be construed in the order listed above.

2. THE PARTIES HEREBY AGREE TO THE FOLLOWING TERMS AND CONDITIONS:

2.1. Duties and Responsibilities

CONTRACTOR agrees to provide the goods and services Bas set forth in this Contract and the above listed documents including any upgrades as outlined in Exhibit B (Scope of Work).

2.2. Delivery and/or Installation.

All deliveries (if provided by the performance of this Contract) are F.O.B. Destination, Prepaid by Supplier, Inside Delivery, as defined by METRO.

METRO shall ensure that all goods delivered are purchased against a Purchase Order and as such METRO assumes no liability for any goods delivered without a purchase order. All deliveries shall be made as defined in the solicitation or purchase order and by the date specified on the purchase order.

Installation, if required, by the solicitation and/or purchase order shall be completed by the date specified on the purchase order. All dates, including those related to deliveries and installation, specified in the purchase order shall be consistent with the mutually agreed dates in the project schedule and/or Exhibit B (Scope of Work).

3. CONTRACT TERM

3.1. Contract Term

The Contract Term will begin on the date (the "Effective Date") this Contract is approved by all required parties and filed in the Metropolitan Clerk's Office. This Contract Term will end thirty-six (36) months from the Effective Date.

This Contract may be extended by a letter signed by both parties. The option to extend may be exercised by, and at the discretion, of the Purchasing Agent. However, in no event shall the term of this Contract exceed sixty (60) months from the Effective Date, unless extended by Contract Amendment

4. COMPENSATION

4.1. Contract Value

This Contract has an estimated value of six million dollars (\$6,000,000.00). The pricing details are included in Exhibit B and are made a part of this Contract by reference. CONTRACTOR shall be paid as work is completed and METRO is accordingly, invoiced according to the payment schedule outlined in Exhibit B.

4.2. Other Fees

There will be no other charges or fees for the performance of this Contract. METRO will make reasonable efforts to make payments within 30 days of receipt of invoice, but in any event shall make payment within 60 days. METRO will make reasonable efforts to make payments to Small Businesses within 15 days of receipt of invoice but in any event shall make payment within 60 days.

4.3. Payment Methodology

Payment in accordance with the terms and conditions of this Contract shall constitute the entire compensation due CONTRACTOR for all goods and/or services provided under this Contract.

METRO will compensate CONTRACTOR in accordance with Exhibit B of this Contract. Subject to these payment terms and conditions, CONTRACTOR shall be paid for delivered/performed products and/or services properly authorized by METRO in accordance with this Contract. Compensation shall be contingent upon the satisfactory provision of the products and/or services as determined by METRO, which shall be in accordance with the mutually agreed acceptance criteria.

4.4. Escalation/De-escalation

This Contract is not eligible for annual escalation/de-escalation adjustments.

4.5. Electronic Payment

All payments shall be effectuated by ACH (Automated Clearing House).

4.6. Invoicing Requirements

CONTRACTOR shall submit invoices for payment in a format acceptable, as described below, to METRO and shall submit invoices no more frequently than monthly for satisfactorily and accurately performed services. CONTRACTOR shall be paid as work is completed and invoices are approved by METRO. The foregoing constitutes an acceptable format, as specified above: Invoices shall detail this Contract Number, Purchase Order Number, line items detailed as provided in the contract, quotes, or SOW milestones, cost and dates of service(s) being billed, accompanied by any necessary supporting documentation as required by METRO. CONTRACTOR shall submit all invoices no later than ninety (90) days after the services have been delivered/performed.

Payment of an invoice by METRO shall not waive METRO's rights of revocation of acceptance due to non-conformity or the difficulty of discovery of the non-conformance. Such revocation of acceptance shall occur within 180 calendar days after METRO discovers or should have discovered the non-conforming product and/or service but prior to any substantial change in condition of the products and/or services caused by METRO.

4.7. Subcontractor/Subconsultant Payments

When payment is received from METRO, CONTRACTOR shall within fourteen (14) calendar days pay all subcontractors, subconsultants, laborers, and suppliers the amounts they are due for the work covered by such payment. Payments can exceed the fourteen (14) calendar days if mutually agreed upon in writing with the subcontractors, subconsultants, laborers, and suppliers. In the event METRO becomes informed that CONTRACTOR has not paid a subcontractor, subconsultant, laborer, or supplier as provided herein, METRO shall have the right, but not the duty, to issue future checks and payments to CONTRACTOR of amounts otherwise due hereunder naming CONTRACTOR and any such subcontractor, subconsultant, laborer, or supplier as joint payees. Such joint check procedure, if employed by METRO, shall create no rights in favor of any person or entity beyond the right of the named payees to payment of the check and shall not be deemed to commit METRO to repeat the procedure in the future. If persistent, this may be determined to be a material breach of this Contract.

5. TERMINATION

5.1. Breach

Should CONTRACTOR fail to fulfill in a timely and proper manner its obligations pursuant to Exhibit B and as specified under this Contract or if it should violate any of the terms of this Contract, METRO shall identify the breach and CONTRACTOR shall cure the performance within thirty (30) days. If CONTRACTOR fails to satisfactorily provide a cure, METRO shall have the right to immediately terminate this Contract. Such termination shall not relieve CONTRACTOR of any liability to METRO for proven damages sustained, and awarded by a court of competent jurisdiction, by virtue of any breach by CONTRACTOR.

Either party may terminate this Contract if the other party neglects or fails to perform or observe any of its material obligations hereunder, including but not limited to timely payment of sums due, and such default continues for forty-five (45) days following receipt of notice.

5.2. Lack of Funding

Should funding for this Contract be discontinued, METRO shall have the right to terminate this Contract immediately upon written notice to CONTRACTOR.

5.3. Notice

METRO may terminate this Contract at any time upon thirty (30) days written notice to CONTRACTOR. Should METRO terminate this Contract, CONTRACTOR shall immediately cease work and deliver to METRO, within thirty (30) days, all completed or partially completed satisfactory, in accordance with the Exhibit B, work, and METRO shall pay to CONTRACTOR the amount due for satisfactory, in accordance with Exhibit B, work performed and deliverables provided in accordance with Exhibit B. For the avoidance of any doubt, the foregoing excludes all pre-existing software, code, utilities, solutions, designs, techniques, methods, methodologies, tools, processes, templates, data, know-how or other materials, information or intellectual property created or developed prior to the Effective Date of this Contract or applicable SOW, whichever date is later, which shall remain the sole and exclusive property of Contractor (or its licensor).

6. NONDISCRIMINATION

6.1. METRO's Nondiscrimination Policy

It is the policy of METRO not to discriminate on the basis of race, creed, color, national origin, age, sex, or disability in its hiring and employment practices, or in admission to, access to, or operation of its programs, services, and activities.

6.2. Nondiscrimination Requirement

No person shall be excluded from participation in, be denied benefits of, be discriminated against in the admission or access to, or be discriminated against in treatment or employment in METRO's contracted programs or activities, on the grounds of race, creed, color, national origin, age, sex, disability, or any other classification protected by federal or Tennessee State Constitutional or statutory law; nor shall they be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of contracts with METRO or in the employment practices of METRO's CONTRACTORS. **CONTRACTOR certifies and warrants that it will comply with this nondiscrimination requirement.** Accordingly, all offerors entering into contracts with METRO shall, upon request, be required to show proof of such nondiscrimination and to post in conspicuous places that are available to all employees and applicants, notices of nondiscrimination.

6.3. Equal Business Opportunity (EBO) Program Requirement

The Equal Business Opportunity (EBO) Program is not applicable to this Contract.

6.4. Covenant of Nondiscrimination

All offerors have committed to the Covenant of Nondiscrimination when registering with METRO to do business. To review this document, go to METRO's website.

7. INSURANCE

7.1. Proof of Insurance

During the term of this Contract, for any and all awards, CONTRACTOR shall, at its sole expense, obtain and maintain in full force and effect for the duration of this Contract, including any extension(s), the types and amounts of insurance identified below. Proof of insurance shall be required naming METRO as additional insured and identifying Contract number on the ACORD document.

7.2. Automobile Liability Insurance

In the amount of one million (\$1,000,000.00) dollars.

7.3. General Liability Insurance

In the amount of one million (\$1,000,000.00) dollars.

7.4. Worker's Compensation Insurance (if applicable)

CONTRACTOR shall maintain workers' compensation insurance with statutory limits required by the State of Tennessee or other applicable laws and Employer's Liability Insurance with limits of no less than one hundred thousand (\$100,000.00) dollars, as required by the laws of Tennessee.

7.5. Cyber Liability Insurance

In the amount of four million (\$4,000,000.00) dollars.

7.6. Technological Errors and Omissions Liability Insurance

In the amount of one million (\$1,000,000.00) dollars.

7.7. Such insurance shall:

Contain or be endorsed to contain a provision that includes METRO, its officials, officers, employees, and volunteers as additional insureds with respect to liability arising out of work or operations performed by or on behalf of CONTRACTOR including materials, parts, or equipment furnished in connection with such work or operations. The coverage shall contain no special limitations on the scope of its protection afforded to the above-listed insureds.

For any claims related to this Contract, CONTRACTOR's insurance coverage shall be primary insurance with respects to METRO, its officers, officials, employees, and volunteers. Any insurance or self-insurance programs covering METRO, its officials, officers, employees, and volunteers shall be in excess of CONTRACTOR's insurance and shall not contribute with it.

Automotive Liability insurance shall include vehicles owned, hired, and/or non-owned. Said insurance shall include coverage for loading and unloading hazards. Insurance shall contain or be endorsed to contain a provision that includes METRO, its officials, officers, employees, and volunteers as additional insureds with respect to liability arising out of automobiles owned, leased, hired, or borrowed by or on behalf of CONTRACTOR. CONTRACTOR shall maintain Workers' Compensation insurance (if applicable) with statutory limits as required by the State of Tennessee or other applicable laws and Employers' Liability insurance. CONTRACTOR shall require each of its subcontractors to provide Workers' Compensation for all of the latter's employees to be engaged in such work unless such employees are covered by CONTRACTOR's Workers' Compensation insurance coverage.

7.8. Other Insurance Requirements

Prior to commencement of services, CONTRACTOR shall furnish METRO with original certificates and amendatory endorsements effecting coverage required by this section and provide that such insurance shall not be cancelled, allowed to expire, or be materially reduced in coverage except on 30 days' prior written notice to:

PROCUREMENTCOI@NASHVILLE.GOV

In the event of a claim or lawsuit, CONTRACTOR shall provide copies of specific endorsements and policies related to the claim or lawsuit if requested by METRO in lieu of or in addition to certificates of insurance.

Replace certificates, , and/or endorsements for any such insurance expiring prior to completion of services.

Maintain such insurance from the time services commence until services are completed. Failure to maintain or renew coverage and to provide evidence of renewal may be treated by METRO as a material breach of this Contract.

Said insurance shall be with an insurer licensed to do business in Tennessee and having A.M. Best Company ratings of no less than A-. Modification of this standard may be considered upon appeal to the METRO Director of Risk Management Services.

Require all subcontractors to maintain during the term of this Contract, Commercial General Liability insurance, Business Automobile Liability insurance, and Worker's Compensation/ Employers Liability insurance (unless subcontractor's employees are covered by CONTRACTOR's insurance) in the same manner as specified for CONTRACTOR. CONTRACTOR shall require subcontractor's to have all necessary insurance and maintain the subcontractor's certificates of insurance.

Any deductibles and/or self-insured retentions greater than \$10,000.00 must be disclosed to and approved by METRO **prior to the commencement of services.**

If CONTRACTOR has or obtains primary and excess policy(ies), there shall be no gap between the limits of the primary policy and the deductible features of the excess policies.

8. GENERAL TERMS AND CONDITONS

8.1. Taxes

METRO is exempt from sales tax and shall not be responsible for any taxes that are imposed on CONTRACTOR. Furthermore, CONTRACTOR understands that it cannot claim exemption from taxes by virtue of any exemption that is provided to METRO.

8.2. Warranty

CONTRACTOR warrants that for a period of one year from date of system Switchover, whichever is later, the goods provided, including software, shall be free of any material defects that interfere with or prohibit the use of the goods for the purposes for which they were obtained.

During the warranty period, METRO may, at its option, request that CONTRACTOR repair or replace any defective goods, by written notice to CONTRACTOR. In that event, CONTRACTOR shall repair or replace the defective goods, as required by METRO, at CONTRACTOR's expense, within thirty (30) days of written notice.

Alternatively, METRO may return the defective goods, at CONTRACTOR's expense, for a full refund for the corresponding defective good. Exercise of either option shall not relieve CONTRACTOR of any liability to METRO for proven damages sustained, and awarded by a court of competent jurisdiction, by virtue of CONTRACTOR's breach of warranty.

8.3. Software License

CONTRACTOR warrants and represents that it is the owner of or otherwise has the right to and does hereby grants METRO a license to use any software provided in accordance with the end user license terms incorporated Exhibit C, for the purposes for which the software was obtained or proprietary material as set forth in METRO's solicitation and/or CONTRACTOR's response to the solicitation.

8.4. Confidentiality

Tennessee Code Annotated § 10-7-504(i) specifies that information which would allow a person to obtain unauthorized access to confidential information or to government property shall be maintained as confidential. "Government property" includes electronic information processing systems, telecommunication systems, or other communications systems of a governmental entity subject to this chapter. Such records include: (A) Plans, security codes, passwords, combinations, or computer programs used to protect electronic information and government property; (B) Information that would identify those areas of structural or operational vulnerability that would permit unlawful disruption to, or interference with, the services provided by a governmental entity; and (C) information that could be used to disrupt, interfere with, or gain unauthorized access to electronic information or government property.

The foregoing listing is not intended to be comprehensive, and any information which a party marks or otherwise designates as anything other than "Public Information" will be deemed and treated as sensitive information, which is defined as any information not specifically labeled as "Public Information". Information which qualifies as "sensitive information" may be presented in oral, written, graphic, and/or machine-readable formats. Regardless of presentation format, such information will be deemed and treated as sensitive information.

Either party, and its affiliates, , may have access to sensitive information. The receiving party, is required to maintain such information in a manner appropriate to its level of sensitivity. All sensitive information must be secured at all times including, but not limited to, the secured destruction of any written or electronic information no longer needed. The unauthorized access, modification, deletion, or disclosure of any confidential information may compromise the integrity and security of a party, violate individual rights of privacy, and/or constitute a criminal act.

Upon the request of by either party, all confidential information shall be returned or a certification of destruction shall be sent to the other party. In the event of any disclosure or threatened disclosure of confidential information, a party is further authorized and entitled to immediately seek and obtain injunctive or other similar relief against the other party, including but not limited to emergency and ex parte relief where available.

8.5. Information Ownership

All METRO information is and shall be the sole property of METRO. CONTRACTOR hereby waives any and all statutory and common law liens it may now or hereafter have with respect to METRO information. Nothing in this Contract or any other agreement between METRO and CONTRACTOR shall operate as an obstacle to such METRO's right to retrieve any and all METRO information from CONTRACTOR or its agents or to retrieve such information or place such information with a third party for provision of services to METRO, including without limitation, any outstanding payments, overdue payments and/or disputes, pending legal action, or arbitration. Upon METRO's request, CONTRACTOR shall supply METRO with an inventory of METRO information that CONTRACTOR stores and/or backs up.

Any information provided to the CONTRACTOR, including information provided by METRO customers or citizens, is only to be used to fulfill the contracted services. Any additional information that is inferred or determined based on primary information that is provided to the CONTRACTOR, i.e. "second-order data", is only to be used to fulfill the contracted services. This information is not to be used for marketing or commercial purposes and the CONTRACTOR asserts no rights to this information outside of fulfilling the contracted services. Storage of this information is not allowed outside United States' jurisdiction.

8.6. Information Security Breach Notification

When applicable, CONTRACTOR shall notify METRO of any data breach involving METRO data within 24 hours of CONTRACTOR's knowledge or reasonable belief (whichever is earlier) that such breach has occurred (Breach Notice) by contacting the METRO ITS Help Desk. The Breach Notice should describe the nature of the breach, the scope of the information compromised, the date the breach occurred, and the identities of the individuals affected or potentially affected by the breach as well as specific information about the data compromised so that METRO can properly notify those individuals whose information was compromised. CONTRACTOR shall periodically update the information contained in the Breach Notice to METRO and reasonably cooperate with METRO in connection with METRO's efforts to mitigate the damage or harm of such breach.

8.7. Virus Representation and Warranty

CONTRACTOR represents and warrants that Products and/or Services, or any media upon which the Products and/or Services are stored, do not have, nor shall CONTRACTOR or its Agents otherwise introduce into METRO's systems, network, or infrastructure, any type of software routines or element which is designed to or capable of unauthorized access to or intrusion upon, disabling, deactivating, deleting, or otherwise damaging or interfering with any system, equipment, software, data, or the METRO network. In the event of a breach of this representation and warranty, CONTRACTOR shall compensate METRO for any and all harm, injury, damages, costs, and expenses incurred by METRO resulting from the breach.

For CONTRACTOR managed systems, CONTRACTOR shall install and maintain ICSA Labs certified or AV-Test approved Antivirus Software and, to the extent possible, use real time protection features. CONTRACTOR shall maintain the Anti-virus Software in accordance with the Antivirus Software provider's recommended practices. In addition, CONTRACTOR shall ensure that:

- Anti-virus Software checks for new Anti-virus signatures no less than once per day, and;
- Anti-virus signatures are current and no less recent than two versions/releases behind the most current version/release of the Anti-virus signatures for the Anti-virus Software

8.8. Copyright, Trademark, Service Mark, or Patent Infringement

CONTRACTOR shall, at its own expense, be entitled to and shall have the duty to defend any suit that may be brought against METRO to the extent that it is based on a third party claim that the products or services furnished infringe a United States Copyright, Trademark, Service Mark, or Patent. CONTRACTOR shall further indemnify and hold harmless METRO against any award of damages and costs made against METRO by a final judgment of a court of last resort in any such suit. METRO shall provide CONTRACTOR immediate notice in writing of the existence of such claim and full right and opportunity to conduct the defense thereof, together with all available information and reasonable cooperation, assistance and authority to enable CONTRACTOR to do so. No costs or expenses shall be incurred for the account of CONTRACTOR without its written consent. METRO reserves the right to participate in the defense of any such action, at its sole expense. CONTRACTOR shall have the right to enter into negotiations for and the right to effect settlement or compromise of any such action, but no such settlement or compromise shall be binding upon METRO unless approved by the METRO Department of Law Settlement Committee and, where required, the METRO Council.

If the products or services furnished under this Contract are likely to, or do become, the subject of such a claim of infringement, then without diminishing CONTRACTOR's obligation to satisfy the final award, CONTRACTOR may at its option and expense:

- Procure for METRO the right to continue using the products or services
- Replace or modify the alleged infringing products or services with other equally suitable products or services that are satisfactory to METRO, so that they become non-infringing
- Remove the products or discontinue the services and cancel any future charges pertaining thereto Provided; however, that CONTRACTOR will not exercise the Remove option above until CONTRACTOR and METRO have determined that the Procure and/or Replace options are impractical. CONTRACTOR shall have no liability to METRO; however, if any such infringement or claim thereof is based upon or arises out of:
 - The use of the products or services in combination with apparatus or devices not supplied or else approved by CONTRACTOR;
 - The use of the products or services in a manner for which the products or services were neither designated nor contemplated; or,
 - The claimed infringement in which METRO has any direct or indirect interest by license or otherwise, separate from that granted herein.

The foregoing provisions state the entire liability and obligations of each party, and the exclusive remedy of the other, with respect to any alleged intellectual property infringement hereunder.

8.9. Maintenance of Records

CONTRACTOR shall maintain documentation for all charges against METRO. The books, records, and documents of CONTRACTOR, insofar as they relate to work performed or money received under this Contract, shall be maintained for a

period of three (3) full years from the date of final payment and will be subject to audit, at any reasonable time and upon reasonable notice by METRO or its duly appointed representatives. The records shall be maintained in accordance with generally accepted accounting principles. In the event of litigation, working papers and other documents shall be produced in accordance with applicable laws and/or rules of discovery. Breach of the provisions of this paragraph is a material breach of this Contract.

All documents and supporting materials related in any manner whatsoever to this Contract or any designated portion thereof, which are in the possession of CONTRACTOR or any subcontractor or subconsultant shall be made available to METRO for inspection and copying upon written request from METRO. Said documents shall also be made available for inspection and/or copying by any state, federal or other regulatory authority, upon request from METRO. Said records include, but are not limited to, all drawings, plans, specifications, submittals, correspondence, minutes, memoranda, tape recordings, videos, or other writings or things which document the procurement and/or performance of this Contract. Said records expressly include those documents reflecting the cost, including all subcontractors' records and payroll records of CONTRACTOR and subcontractors.

8.10. Monitoring

CONTRACTOR's activities conducted and records maintained pursuant to this Contract shall be subject to monitoring and evaluation by METRO, the Department of Finance, the Division of Internal Audit, or their duly appointed representatives.

METRO shall have the option of reviewing and performing a security assessment of the information security management practices of CONTRACTOR..

8.11. METRO Property

Any METRO property, including but not limited to books, records, and equipment that is in CONTRACTOR's possession shall be maintained by CONTRACTOR in good condition and repair, and shall be returned to METRO by CONTRACTOR upon termination of this Contract. All goods, documents, records, and other work product and property produced specifically for METRO during the performance of this Contract are deemed to be METRO property. METRO property includes, but is not limited to, all documents which make up this Contract; all other documents furnished by METRO; all goods, records, reports, information, data, specifications, computer programs, technical reports, operating manuals and similar work or other documents, conceptual drawings, design documents, closeout documents, and other submittals by CONTRACTOR of any of its subcontractors; and, all other original works of authorship, whether created by METRO, CONTRACTOR or any of its subcontractors embodied in any tangible medium of expression, including, without limitation, pictorial, graphic, sculptural works, two (2) dimensional works, and three (3) dimensional works..

Except as to Contracts involving sensitive information, CONTRACTOR may keep one (1) copy of the aforementioned documents upon completion of this Contract; provided, however, that in no event shall CONTRACTOR use, or permit to be used, any portion of the documents on other projects without METRO's prior written authorization. CONTRACTOR shall maintain sensitive information securely and if required by METRO, provide secured destruction of said information. Distribution and/or reproduction of METRO sensitive information outside of the intended and approved use are strictly prohibited unless permission in writing is first received from the METRO Chief Information Security Officer. The storage of METRO sensitive information to third-party hosted network storage areas, such as Microsoft Skydrive, Google Docs, Dropbox, or other cloud storage mechanisms, shall not be allowed without first receiving permission in writing from the METRO Chief Information Security Officer.

8.12. Modification of Contract

This Contract may be modified only by written amendment executed by all parties and their signatories hereto. All change orders, where required, shall be executed in conformance with section 4.24.020 of the Metropolitan Code of Laws.

8.13. Partnership/Joint Venture

This Contract shall not in any way be construed or intended to create a partnership or joint venture between the Parties or to create the relationship of principal and agent between or among any of the Parties. None of the Parties hereto shall hold itself out in a manner contrary to the terms of this paragraph. No Party shall become liable for any representation, act, or omission of any other Party contrary to the terms of this Contract.

8.14. Waiver

No waiver of any provision of this Contract shall affect the right of any Party to enforce such provision or to exercise any right or remedy available to it.

8.15. Employment

CONTRACTOR shall not subscribe to any personnel policy which permits or allows for the promotion, demotion, employment, dismissal or laying off of any individual due to race, creed, color, national origin, age, sex, or which is in violation of applicable laws concerning the employment of individuals with disabilities.

CONTRACTOR shall not knowingly employ, permit, dispatch, subcontract, or instruct any person who is an undocumented and/or unlawful worker to perform work in whole or part under the terms of this Contract.

Violation of either of these contract provisions may result in suspension or debarment if not resolved in a timely manner, not to exceed ninety (90) days, to the satisfaction of METRO.

8.16. Compliance with Laws

CONTRACTOR agrees to comply with all applicable federal, state and local laws and regulations.

8.17. Iran Divestment Act

In accordance with the Iran Divestment Act, Tennessee Code Annotated § 12-12-101 et seq., CONTRACTOR certifies that to the best of its knowledge and belief, neither CONTRACTOR nor any of its subcontractors are on the list created pursuant to Tennessee Code Annotated § 12-12-106. Misrepresentation may result in civil and criminal sanctions, including contract termination, debarment, or suspension from being a contractor or subcontractor under METRO contracts.

8.18. Boycott of Israel

The Contractor certifies that it is not currently engaged in, and will not for the duration of the contract engage in, a boycott of Israel as defined by Tenn. Code Ann. § 12-4-119. This provision shall not apply to contracts with a total value of less than two hundred fifty thousand dollars (\$250,000) or to contractors with less than ten (10) employees.

8.19. Taxes and Licensure

CONTRACTOR shall have all applicable licenses and be current on its payment of all applicable gross receipt taxes and personal property taxes.

8.20. Ethical Standards

It shall be a breach of the Ethics in Public Contracting standards in the Metropolitan Code of Laws for any person to offer, give or agree to give any employee or former employee, or for any employee or former employee to solicit, demand, accept or agree to accept from another person, a gratuity or an offer of employment in connection with any decision, approval, disapproval, recommendation, preparation of any part of a program requirement or a purchase request, influencing the content of any specification or procurement standard, rendering of advice, investigation, auditing or in any other advisory capacity in any proceeding or application, request for ruling, determination, claim or controversy or other particular matter, pertaining to any program requirement of a contract or subcontract or to any solicitation or proposal therefore. It shall be a breach of the Ethics in Public Contracting standards for any payment, gratuity or offer of employment to be made by or on behalf of a subcontractor under a contract to the prime contractor or higher tier subcontractor or a person associated therewith, as an inducement for the award of a subcontract or order. Breach of the provisions of this paragraph is, in addition to a breach of this contract, a breach of ethical and legal standards which may result in civil or criminal sanction and/or debarment or suspension from being a contractor or subcontractor under METRO contracts.

Contract 6543886

Pursuant to Metropolitan Code of Laws, Section 4.48.020, entities and persons doing business with, or proposing to do business with, the Metropolitan Government of Nashville & Davidson County must adhere to the ethical standards prescribed in Section 4.48 of the Code. By signing this contract, you agree that you have read the standards in Section 4.48 and understand that you are obligated to follow them. Violation of any of those standards is a breach of contract and a breach of legal standards that may result in sanctions, including those set out in Section 4.48.

8.21. Indemnification and Hold Harmless

CONTRACTOR shall indemnify and hold harmless METRO, its officers, agents, and employees from:

A. Any claims, damages, costs, and attorney fees for injuries or damages arising, in part or in whole, from the negligent or intentional acts or omissions of CONTRACTOR, its officers, employees, and/or agents, including its sub or independent contractors, in connection with the performance of the contract.

B. Any claims, damages, penalties, costs, and attorney fees arising from any failure of CONTRACTOR, its officers, employees, and/or agents, including its sub or independent contractors, to observe applicable laws, including, but not limited to, labor laws and minimum wage laws.

C. METRO will not indemnify, defend, or hold harmless in any fashion CONTRACTOR from any claims arising from any failure, regardless of any language in any attachment or other document that CONTRACTOR may provide.

LIMITATION OF LIABILITY. To the extent permitted by Tennessee law, the foregoing limitation of liability shall not apply to claims for intentional torts, criminal acts, fraudulent conduct, or acts or omissions that result in personal injuries or death and shall not waive or limit the state's legal rights, sovereign immunity, or any other immunity from suit provided by law. IN NO EVENT SHALL NEC'S MAXIMUM LIABILITY FOR ALL DAMAGES RELATED TO THE SERVICES PURCHASED HEREUNDER OR OTHERWISE ARISING IN CONNECTION HERewith EXCEED THE TOTAL VALUE OF THIS CONTRACT DURING THE CONTRACT TERM TO THE EXTENT PERMITTED BY TENNESSEE LAW.

TO THE EXTENT PERMITTED BY TENNESSEE LAW, IN NO EVENT SHALL CONTRACTOR BE LIABLE TO METRO FOR (I) ANY SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES WHETHER FORESEEABLE OR UNFORESEEABLE WHICH MAY ARISE IN CONNECTION WITH THIS CONTRACT.

8.22. Attorney Fees

CONTRACTOR agrees that in the event either party takes legal action to enforce any provision of this Contract or to obtain a remedy for any breach of this Contract, and in the event METRO prevails in such action, CONTRACTOR shall pay all expenses of such action incurred at any and all stages of the litigation, including costs, and reasonable attorney fees for METRO. In the event CONTRACTOR prevails in such action that METRO will be responsible for their own expenses of such action incurred.

8.23. Assignment--Consent Required

The provisions of this Contract shall inure to the benefit of and shall be binding upon the respective successors and assignees of the parties hereto. Except for the rights of money due to CONTRACTOR under this Contract, neither this Contract nor any of the rights and obligations of CONTRACTOR hereunder shall be assigned or transferred in whole or in part without the prior written consent of METRO. Any such assignment or transfer shall not release CONTRACTOR from its obligations hereunder.

Contract 6543886

NOTICE OF ASSIGNMENT OF ANY RIGHTS TO MONEY DUE TO CONTRACTOR UNDER THIS CONTRACT MUST BE SENT TO THE ATTENTION OF:

PRG@NASHVILLE.GOV (Preferred Method)

OR

METRO'S PURCHASING AGENT

PROCUREMENT DIVISION

DEPARTMENT OF FINANCE

PO BOX 196300

NASHVILLE, TN 37219-6300

Funds Assignment Requests should contain complete contact information (contact person, organization name, address, telephone number, and email) for METRO to use to request any follow up information needed to complete or investigate the requested funds assignment. To the extent permitted by law, METRO has the discretion to approve or deny a Funds Assignment Request.

8.24. Entire Contract

This Contract sets forth the entire agreement between the parties with respect to the subject matter hereof and shall govern the respective duties and obligations of the parties.

8.25. Force Majeure

No party shall have any liability to the other hereunder by reason of any delay or failure to perform any obligation or covenant if the delay or failure to perform is occasioned by *force majeure*, meaning any act of God, storm, fire, casualty, unanticipated work stoppage, strike, lockout, labor dispute, civil disturbance, riot, war, national emergency, act of Government, act of public enemy, or other cause of similar or dissimilar nature beyond its control.

8.26. Governing Law

The validity, construction, and effect of this Contract and any and all extensions and/or modifications thereof shall be governed by the laws of the State of Tennessee. Tennessee law shall govern regardless of any language in any attachment or other document that CONTRACTOR may provide.

8.27. Venue

Any action between the Parties arising from this Contract shall be maintained in the courts of Davidson County, Tennessee.

8.28. Severability

Should any provision of this Contract be declared to be invalid by any court of competent jurisdiction, such provision shall be severed and shall not affect the validity of the remaining provisions of this Contract.

[BALANCE OF PAGE IS INTENTIONALLY LEFT BLANK]

Contract Number: 6543886

Notices and Designation of Agent for Service of Process

All notices to METRO shall be mailed or hand delivered to:

**PURCHASING AGENT
PROCUREMENT DIVISION
DEPARTMENT OF FINANCE
PO BOX 196300
NASHVILLE, TN 37219-6300**

Notices to CONTRACTOR shall be mailed or hand delivered to:

CONTRACTOR: NEC Corproation of America

Attention: Contracts Department

Address: 3929 W John Carpenter Fwy, Irving, TX 75063

Telephone: (214)-262-6000

Fax: N/A

E-mail: necamcontracts@necam.com

CONTRACTOR designates the following as the CONTRACTOR's agent for service of process and will

waive any objection to service of process if process is served upon this agent:

Designated Agent: National Registered Agents, Inc

Attention: N/A

Address: 300 Montvue Rd, Knoxville, TN 37919-5546

Email: N/A

[SPACE INTENTIONALLY LEFT BLANK]

Notices & Designations
Department & Project Manager

Contract Number	6543886
------------------------	---------

The primary DEPARTMENT/AGENCY responsible for the administration of this contract is:

DEPARTMENT	Police
Attention	John Singleton
Address	600 Murfreesboro Pike P.O. Box 196399 Nashville, TN 37219-6399
Telephone	616-862-7702
Email	john.singleton@nashville.gov

The primary DEPARTMENT/AGENCY responsible for the administration of this contract designates the following individual as the PROJECT MANAGER responsible for the duties outlined in APPENDIX – Z CONTRACT ADMINISTRATION:

Project Manager	Kristin Heil
Title	IT Manager
Address	600 Murfreesboro Pike P.O. Box 196399 Nashville, TN 37219-6399
Telephone	(615) 862-7110
Email	kristin.heil@nashville.gov

Appendix Z – Contract Administration

Upon filing with the Metropolitan Clerk, the PROJECT MANAGER designated by the primary DEPARTMENT/AGENCY is responsible for contract administration. Duties related to contract administration include, but are not necessarily limited to, the following:

Vendor Performance Management Plan

For contracts in excess of \$50,000.00, the project manager will develop a vendor performance management plan. This plan is managed by the primary department/agency and will be retained by the department/agency for their records. At contract close out, copies of all vendor performance management documents will be sent to PRG@nashville.gov.

For best practices related to vendor performance management, project managers will consult chapter eight of the PROCUREMENT MANUAL found on the division of purchases internal resources page: <https://metronashville.sharepoint.com/sites/IMFinanceProcurement>.

Amendment

For all contracts, the project manager will notify PRG@nashville.gov if changes to the term, value, scope, conditions, or any other material aspect of the contract are required. The email notification will include a complete CONTRACT AMENDMENT REQUEST FORM found on the division of purchases internal resources page: <https://metronashville.sharepoint.com/sites/IMFinanceProcurement>.

Escalation

For contracts that include an escalation/de-escalation clause, the project manager will notify PRG@nashville.gov when any request for escalation/de-escalation is received. The email notification will include any documentation required by the contract to support the request.

Contract Close Out – Purchasing

For all contracts, the project manager will notify PRG@nashville.gov when the work is complete and has been accepted by the department/agency. The email notification will include the contract number, contract title, date of completion, warranty start date and warranty end date (if applicable), and copies of all vendor performance management documents (if applicable).

Contract Close Out – BAO

For contracts with compliance monitored by the Business Assistance Office (BAO), the project manager will notify the designated contract compliance officer via email when the contract is complete and final payment has been issued. The email notification will include the contract number, contract title, and the date final payment was issued.

Best Practices

Project managers are strongly encouraged to consult chapter eight of the PROCUREMENT MANUAL for best practices related to contract administration. The manual is found on the division of purchases internal resources page:

<https://metronashville.sharepoint.com/sites/IMFinanceProcurement>

Contract Number 6543886

Effective Date

This contract shall not be binding upon the parties until it has been fully electronically approved by the CONTRACTOR, the authorized representatives of the Metropolitan Government, and filed in the office of the Metropolitan Clerk.

THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

APPROVED AS TO PROJECT SCOPE:

Chief of Police John Drake SM
Dept. / Agency / Comm. Head or Board Chair. Dept. Fin.

APPROVED AS TO COMPLIANCE WITH PROCUREMENT CODE:

Dennis Rowland DR
Purchasing Agent Purchasing

APPROVED AS TO AVAILABILITY OF FUNDS:

Kevin Crumbolmal EF
Director of Finance BA

APPROVED AS TO FORM AND LEGALITY:

Jessie Ortiz-Marsh BL
Metropolitan Attorney Insurance

FILED BY THE METROPOLITAN CLERK:

Metropolitan Clerk Date

CONTRACTOR:

NEC Corporation of America
Company Name

Eugene LeRoux
Signature of Company's Contracting Officer

Eugene LeRoux
Officer's Name

Senior Vice President
Officer's Title

Exhibit A – MISA Terms and Conditions**Contract 6543886****EXHIBIT A- MISA Terms and Conditions****SECTION A-1****General Terms and Conditions**

- 1 Safeguards.** In addition to the controls specified in the exhibits to this Agreement, Contractor agrees to implement administrative, physical, and technical safeguards to protect the availability, confidentiality and integrity of Metropolitan Government of Nashville and Davison County (Metro Government) Information, information technology assets and services. All such safeguards shall be in accordance with industry-wide best security practices and commensurate with the importance of the information being protected, but in no event less protective than those safeguards that Contractor uses to protect its own information or information of similar importance, or is required by applicable federal or state law.
- 2 Inventory.** Contractor agrees to maintain at all times during the Term of this Agreement a Product and Service Inventory. Contractor shall upon request of Metro Government, which shall be no more frequently than semi-annually, provide the current Product and Service Inventory to Metro Government within thirty (30) days of the request.
- 3 Connection of Systems or Devices to the Metro Government Network.** Contractor shall not place any systems or devices on the Metro Government Network without the prior written permission of the Director of ITS, designee, or the designated Metro Government contact for this Agreement.
- 4 Access Removal.** If granted access to Metro Government Network or systems, Contractor and its Agents shall only access those systems, applications or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass security controls. Notwithstanding anything to the contrary in the Purchasing Agreement or other agreement between Metro Government and Contractor, Metro Government at its sole discretion, may refuse granting access right to Metro Government Network or Sensitive Information to any Agent of Contractor, and may at any time remove access rights (whether physical premise access or system access) from Contractor or any Agents, without prior notice or liability to Contractor, if Metro Government reasonably suspects a security violation by Contractor or such Agent or otherwise deems such action appropriate to protect Metro Government Infrastructure, Metro Government Network or Metro Government Information.
- 5 Subcontracting/Outsourcing.**
 - 5.1 Prior Approval.** Without Metro Government's prior written consent, Contractor may not subcontract with a third party to perform any of its obligations to Metro Government which involves access to Metro Government Information or connection to Metro Government Network. Nor shall Contractor outsource any Contractor infrastructure (physical or virtual) which Stores Sensitive Information without such consent. To obtain Metro Government's consent, Contractor shall contact the Metro Government ITS department. In addition, Metro Government may withdraw any prior consent if Metro Government reasonably suspect a violation by the subcontractor or outsource provider of this Agreement, or otherwise deems such withdraw necessary or appropriate to protect Metro Government Network, Metro Government Infrastructure or Metro Government Information.
 - 5.2 Subcontractor Confidentiality.** Contractor Agents are bound by the same confidentiality obligations set forth in this Agreement. Contractor or its Agent may not transfer, provide access to or otherwise make available Metro Government Information to any individual or entity outside of the United States (even within its own organization) without the prior written consent of Metro Government. To obtain such consent, Contractor shall send Metro Government a notice detailing the type of information to be disclosed, the purpose of the disclosure, the recipient's identification and location, and other information required by Metro Government.
 - 5.3 Contractor Responsibility.** Prior to subcontracting or outsourcing any Contractor's obligations to Metro Government, Contractor shall enter into a binding agreement with its subcontractor or outsource service provider ("Third Party Agreement") which (a) prohibits such third party to further subcontract any of its obligations, (b) contains provisions no less protective to Metro Government Network, Metro Government Infrastructure and/or Metro Government Information than those in this Agreement, and (c) expressly provides Metro Government the right to audit such subcontractor or outsource service provider to the same extent that Metro Government may audit Contractor under this Agreement. Contractor warrants that the Third Party Agreement will be enforceable by Metro Government in the U.S. against the subcontractor or outsource provider (e.g., as an intended third party beneficiary under the Third Party Agreement).

Exhibit A – MISA Terms and Conditions

Contract 6543886

Without limiting any other rights of Metro Government in this Agreement, Contractor remains fully responsible and liable for the acts or omissions of its Agents. In the event of an unauthorized disclosure or use of Sensitive Information by its Agent, Contractor shall, at its own expense, provide assistance and cooperate fully with Metro Government to mitigate the damages to Metro Government and prevent further use or disclosure.

SECTION A-2**Definitions**

Capitalized terms used in the Agreement shall have the meanings set forth in this Exhibit A-2 or in the [Metropolitan Government Information Security Glossary](#), which can be found on the Metropolitan Government of Nashville website . Terms not defined in this Exhibit A-2 or otherwise in the Agreement shall have standard industry meanings.

1. “Affiliates” as applied to any particular entity, means those entities, businesses, and facilities that are controlled by, controlling, or under common control with a stated entity, as well as (with respect to Metro Government) any entity to which Metro Government and/or any of the foregoing provides information processing services.
2. “Agent” means any subcontractor, independent contractor, officer, director, employee, consultant or other representative of Contractor, whether under oral or written agreement, whether an individual or entity.
3. “Agreement” means this Information Security Agreement, including all applicable exhibits, addendums, and attachments.
4. “Information Breach” means any actual or suspected unauthorized disclosure or use of, or access to, Metro Government Information, or actual or suspected loss of Metro Government Information.
5. “Effective Date” means the date first set forth on page 1 of the Agreement.
6. “Metro Government Information” means an instance of an information type belonging to Metro Government. Any communication or representation of knowledge, such as facts, information, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual, owned by or entrusted to Metro Government.
7. “Metro Government Infrastructure” means any information technology system, virtual or physical, which is owned, controlled, leased, or rented by Metro Government, either residing on or outside of the Metro Government Network. Metro Government Infrastructure includes infrastructure obtained from an IAAS provider or systems that are provided and located on the Metro Government Network as part of a Service.
8. “Metro Government Network” means any Wide Area Network (WAN) or Local Area Network (LAN) owned, operated, managed or controlled by Metro Government.
9. “Term” means the period during which this Agreement is in effect.

SECTION AST**Agent Security and Training**

- 1 Background Check.** Contractor shall perform a background check which includes a criminal record check on all Agents, who may have access to Metro Government Information. Contractor shall not allow any Agents to access Metro Government Information or perform Services under a Purchasing Agreement if Contractor knows or reasonably should know that such Agent has been convicted of any felony or has been terminated from employment by any employer or contractor for theft, identity theft, misappropriation of property, or any other similar illegal acts.
- 2 Information Security Officer.** If Agents will access or handle Metro Government Information, Contractor shall designate an Information Security Officer, who will be responsible for Contractor information security and compliance with the terms of this Agreement as it relates to Metro Government Information.
- 3 Agent Access Control.** Contractor shall implement and maintain procedures to ensure that any Agent who accesses Metro Government Information has appropriate clearance, authorization, and supervision. These procedures must include:
 - 3.1** Documented authorization and approval for access to applications or information stores which contain Metro Government Information; e.g., email from a supervisor approving individual access (note: approver should not also have technical rights to grant access to Sensitive Information); documented role-based access model; and any equivalent process which retains documentation of access approval.
 - 3.2** Periodic (no less than annually) reviews of Agent user access rights in all applications or information stores which contain Sensitive Information. These reviews must ensure that access for all users is up-to-date, appropriate and approved.
 - 3.3** Termination procedures which ensure that Agent's user accounts are promptly deactivated from applications or information stores which contain Sensitive Information when users are terminated or transferred. These procedures must ensure that accounts are deactivated or deleted no more than 14 business days after voluntary termination, and 24 hours after for cause terminations.
 - 3.4** Procedures which ensure that Agent's user accounts in applications or information stores which contain Sensitive Information are disabled after a defined period of inactivity, no greater than every 180 days.
 - 3.5** Procedures which ensure that all Agents use unique authentication credentials which are associated with the Agent's identity (for tracking and auditing purposes) when accessing systems which contain Sensitive Information.
 - 3.6** Contractor will maintain record of all Agents who have been granted access to Metro Government Sensitive Information. Contractor agrees to maintain such records for the length of the agreement plus 3 years after end of agreement. Upon request, Contractor will supply Metro Government with the names and login IDs of all Agents who had or have access to Metro Government Information.
- 4 Agent Training.**
 - 4.1** Contractor shall ensure that any Agent who access applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of the information or information and the security of the application. Completion of this training must be documented and must occur before Agent may access any Sensitive Information. This training must include, at a minimum:
 - 4.1.1** Appropriate identification and handling of Metro Government Information

Exhibit A – MISA Terms and Conditions**Contract 6543886**

- 4.1.1.1 Awareness of confidentiality requirements contained in this Agreement;
 - 4.1.1.2 Procedures for encrypting Metro Government Information before emailing or transmitting over an Open Network, if the information classification of the information requires these controls;
 - 4.1.1.3 Procedures for information storage on media or mobile devices (and encrypting when necessary).
 - 4.1.2** Education about the procedures for recognizing and reporting potential Information Security Incidents;
 - 4.1.3** Education about password maintenance and security (including instructions not to share passwords);
 - 4.1.4** Education about identifying security events (e.g., phishing, social engineering, suspicious login attempts and failures);
 - 4.1.5** Education about workstation and portable device protection; and
 - 4.1.6** Awareness of sanctions for failing to comply with Contractor security policies and procedures regarding Sensitive Information.
 - 4.1.7** Periodic reminders to Agents about the training topics set forth in this section.
- 4.2** Contractor shall ensure that any Agent who accesses applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of this information. Completion of this training must be documented and must occur before Agent may access any Metro Government Information. This training must include, at a minimum:
- 4.2.1** Instructions on how to identify Metro Government Information.
 - 4.2.2** Instructions not to discuss or disclose any Sensitive Information to others, including friends or family.
 - 4.2.3** Instructions not to take media or documents containing Sensitive Information home unless specifically authorized by Metro Government to do so.
 - 4.2.4** Instructions not to publish, disclose, or send Metro Government Information using personal email, or to any Internet sites, or through Internet blogs such as Facebook or Twitter.
 - 4.2.5** Instructions not to store Metro Government Information on any personal media such as cell phones, thumb drives, laptops, personal digital assistants (PDAs), unless specifically authorized by Metro Government to do so as part of the Agent's job.
 - 4.2.6** Instructions on how to properly dispose of Metro Government Information, or media containing Metro Government Information, according to the terms in Exhibit DMH as well as applicable law or regulations.
- 5 Agent Sanctions.** Contractor agrees to develop and enforce a documented sanctions policy for Agents who inappropriately and/or in violation of Contractor's policies and this Agreement, access, use or maintain applications or information stores which contain Sensitive Information. These sanctions must be applied consistently and commensurate to the severity of the violation, regardless of level within management, and including termination from employment or of contract with Contractor.

SECTION AV

Protection Against Malicious Software

- 1 **Microsoft Systems on Metro Government Networks.** For Products which will be installed on Microsoft Windows Systems residing on Metro Government Network, Contractor warrants that the Product will operate in conjunction with Metropolitan Government Antivirus Software.

- 2 **Non-Microsoft Systems on Metro Government Networks.** For Products installed on non-Microsoft Windows Systems residing on Metro Government Network, Contractor shall allow Metro Government to install Antivirus Software on such Products where technically possible. Upon Metro Government's request, Contractor shall provide the requisite information to implement such Antivirus Software in a manner which will not materially impact the functionality or speed of the Product.

SECTION BU**Information Backup, Contingency Planning and Risk Management****1 General.**

- 1.1** Contractor agrees to backup Metro Government Information which Contractor maintains or Stores. Backup and restoration procedures and related infrastructure, including frequency of backup, offsite storage, media lifespan and media reliability, must be commensurate with the criticality and availability requirement of the Metro Government Information being backed up.
 - 1.2** Upon Metro Government's request, Contractor shall supply Metro Government with an inventory of Metro Government Information that Contractor Stores and/or backed up.
 - 1.3** Contractor shall periodically, no less often than annually, test backup tapes or media by restoring Metro Government Information to a system similar to the original system where the Metro Government Information are stored.
 - 1.4** Upon Metro Government's request, Contractor shall supply copies of Metro Government Information in a format requested by Metro Government.
 - 1.5** Contractor shall backup business critical information at a frequency determined by Metro Government business owner.
- 2 Storage of Backup Media.** Contractor shall store archival and backup media in a secured offsite location. Upon request, Contractor will promptly notify Metro Government of the physical address of the offsite location. The backups of the information should be stored in a manner commiserate with the security around the information. The backup tapes should be encrypted if the sensitivity of the information requires that level of security.
- 3 Disaster Recovery Plan.** Contractor will maintain a Disaster Recovery Plan for all applications or information stores which contain business critical information. This plan will outline the procedures necessary to restore business critical information on the application or systems in a timely fashion in the case of an emergency or disaster.
- 4 Emergency Mode Operation Plan.** Contractor shall maintain an emergency mode operating plan which ensures that systems or applications using or accessing business critical information are operational during an emergency or natural disaster, or are made operational after a disaster in a prompt manner, commensurate with the criticality of the information on the system.
- 5 Testing and Revision Procedure.** Contractor agrees to test, at least annually, Contractor Disaster Recovery Plan and emergency mode operations plan and maintain a documented procedure for such testing. Contractor shall document the results and findings from such testing and revise the plan accordingly.
- 6 Risk Management Requirements.** Contractor shall implement internal risk management practices to ensure the confidentiality, integrity and availability of Metro Government Information within the scope of the SOW. These practices will be no less secure than the ones used by Contractor to protect Contractor's own Sensitive Information or information of comparable sensitivity.

SECTION CSP**Cloud Service Providers****1 Certifications and Compliance.**

- 1.1. Contractor will, on at least an annual basis, hire a third party auditing firm to perform a Statement on Standards for Attestation Engagements (SSAE) No. 16 audit, or equivalent audit, on internal and external Contractor procedures and systems that access or contain Metro Data.
- 1.2. Contractor shall adhere to SOC 1/SSAE 16 audit compliance criteria and data security procedures (or any successor report of a similar nature that is generally accepted in the industry and utilized by Contractor) applicable to Contractor. Upon Metro's request, Contractor will provide Metro with a copy of the audit results set forth in Contractor's SOC 1/SSAE 16 audit report.
- 1.3. Metro shall have the right to terminate this Agreement (together with any related agreements, including licenses and/or Statement(s) of Work) and receive a full refund for all monies prepaid thereunder in the event that the Contractor fails to produce an acceptable SSAE-16/ SOC-1 Type II report.
- 1.4. The Contractor will ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act) 44 U.S.C. § 3541, et seq.), 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 Metro with any documentation it requires for its reporting requirements within 10 days of a request.
- 1.5. Contractor agrees to comply with all applicable privacy laws.

2 **Data Security.** Metro data, including but not limited to data hosted, stored, or held by the Contractor in the Product(s) or in the platform operated by Contractor, or on any device owned or in the custody of Contractor, its employees, agents or Contractors, will be encrypted. Contractor will not transmit any unencrypted Metro Data over the internet or a wireless network, and will not store any Metro Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software approved by Metro.

3 **Use of Subcontractors.** The Contractor shall retain operational configuration and control of data repository systems used to process and store Metro data to include any or remote work. In the event that the Contractor has subcontract the operational configuration and control of any Metro data, Contractor is responsible for ensuring that any third parties that provide services to the Contractor meets security requirements that the Contractor has agreed upon in this contract.

4 **Location of Data.** The Contractor shall maintain all data within the United States, which means the 50 States, the District of Columbia, and outlying areas. The Contractor shall provide Metro with a list of the physical locations that may contain Metro data within 20 days with updates on a quarterly basis.

5 **Personnel Access.** The Contractor will require all employees who will have access to Metro data, the architecture that supports Metro data, or any physical or logical devices/code to pass an appropriate background investigation.

6 Asset Availability.

- 6.1. The Contractor must inform Metro of any interruption in the availability of the cloud service as required by the agreed upon service level agreement. Whenever there is an interruption in service, the Contractor must inform Metro of the estimated time that the system or data will be unavailable. The Contractor must provide regular updates to Metro on the status of returning the service to an operating state according to any agreed upon SLAs and system availability requirements.
- 6.2. The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with Metro'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 timely notification to Metro and shall be responsible for working with Metro to identify appropriate remedies and if applicable, work with Metro to facilitate a smooth and seamless transition to an alternative solution and/or provider.

7 Misuse of Metro Data and Metadata.

- 7.1. The Contractor shall not access, use, or disclose Metro data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Metro data shall only be for purposes specified in this contract or task order. Contractor shall ensure

Exhibit A – MISA Terms and Conditions**Contract 6543886**

that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Metro data, sign a contract or task order specific nondisclosure agreement.

- 7.2. The Contractor shall use Metro-related data only to manage the operational environment that supports Metro data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer. A breach of the obligations or restrictions may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by the breach.

8 Data Breach and Incident Reporting.

- 8.1. The Contractor will submit reports of cyber incidents through approved reporting mechanisms. The Contractor's existing notification mechanisms that are already in place to communicate between the Contractor and its customers may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.
- 8.2. The Contractor will use a template format when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.
- 8.3. In addition to the above, if the incident concerns a breach of PII or a potential breach of PII, the Contractor will report to the contracting officer's designee within 24 hours of the discovery of any data breach. The Contractor shall provide Metro with all information and cooperation necessary to enable compliance by the Contractor and/or Metro with data breach reporting and mitigation actions required by applicable law, regulation, policy, and this contract.

- 9 **Facility Inspections.** The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by Metro, conduct a security audit based on Metro's criteria as needed, but no more than once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with Metro within 20 days of the Contractor's receipt of the audit results.

10 Law Enforcement.

- 10.1. The Contractor shall record all physical access to the cloud storage facilities and all logical access to Metro data. This may include the entrant's name, role, purpose, account identification, entry and exit time.
- 10.2. If Metro data is co-located with the non-Metro data, the Contractor shall isolate Metro data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Metro personnel identified by the Metro personnel, and without the Contractor's involvement.

- 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 prevent proactively 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, with special emphasis on assuring that the vendor's PVM systems and programs apply standardized configurations with automated continuous monitoring of the same 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 Metro are compatible with existing systems and architecture of Metro.

- 12 **Notification.** The Contractor shall notify Metro within 60 minutes of any warrants, seizures, or subpoenas it receives that could result in the loss or unauthorized disclosure of any Metro data. The Contractor shall cooperate with Metro to take all measures to protect Metro data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.

- 13 **Supply Chain.** The Contractor is responsible for exercising due diligence to use genuine hardware and software products that are free of malware.

- 14 **Service Level Agreements.** The Contractor shall work with Metro to develop a service level agreement, including defining roles, responsibilities, terms, and clear measures for performance by Contractor

SECTION DEV**Development**

- 1 Source Code License/Source Code Escrow.** Source code is to be provided to either Metro Government or an escrow agent as a deliverable of any software development project or any other projects which requires code to be created as a deliverable and after any updates to code. CONTRACTOR must provide proof that all source code provided to Metro Government or to escrow agent is complete, up to date and includes all components necessary to function in production environment. Said source code shall be considered the Confidential Information of CONTRACTOR or its successor and Metro Government may only use, copy and/or modify the source code consistent with the purposes of this agreement.
 - 1.1 Source Code License.** CONTRACTOR agrees to provide Metro Government a source code license and will provide, as part of deliverable, source code that is developed as part of this contract, including any customizations. Source code to be provided in an agreed upon media and will be provided within 30 days after any updates. Any third party libraries used in the development of the software will also be included. Documentation provided must be sufficient for a developer versed in the applicable programming language to fully understand source code.
 - 1.2 Source Code Escrow.** In the event that (i) CONTRACTOR becomes insolvent or bankrupt, (ii) CONTRACTOR makes an assignment for the benefit of creditors, (iii) CONTRACTOR consents to a trustee or receiver appointment, (iv) a trustee or receiver is appointed for CONTRACTOR or for a substantial part of its property without its consent, (v) CONTRACTOR voluntarily initiates bankruptcy, insolvency, or reorganization proceedings, or is the subject of involuntary bankruptcy, insolvency, or reorganization proceedings, or (vi) CONTRACTOR announces that it has entered into an agreement to be acquired by a then named Competitor, then CONTRACTOR will negotiate in good faith to enter into a source code escrow agreement with a mutually agreed source code escrow company setting forth source code escrow deposit procedures and source code release procedures relating to the software provided as part of this contract. Notwithstanding the foregoing, the escrow instructions shall provide for a release of the source code to Metro Government only upon the occurrence of (a) the filing of a Chapter 7 bankruptcy petition by CONTRACTOR, or a petition by CONTRACTOR to convert a Chapter 11 filing to a Chapter 7 filing; (b) the cessation of business operations by CONTRACTOR; or (c) the failure on the part of CONTRACTOR to comply with its contractual obligations to Metro Government to comply with its maintenance and support obligations for a period of more than thirty (30) days after it has received written notice of said breach. In the event of a release of source code pursuant to this section, said source code shall continue to be the Confidential Information of CONTRACTOR or its successor in interest. In the event of a release of source code to Metro Government from escrow, Metro Government may only use, copy and/or modify the source code consistent with the purposes of this agreement (or have a contractor who has agreed in writing to confidentiality provisions as restrictive as those set forth in this Agreement do so on its behalf).
- 2 Mobile Applications Security.** CONTRACTOR shall have the ability/expertise to develop secure mobile applications. Specifically, an awareness of secure mobile application development standards, such as OWASP's Mobile Security project. Development should be able to meet at a minimum OWASP's MASVS-L1 security standard or a similar set of baseline security standards as agreed upon by Metro Government.

SECTION DMH**Device and Storage Media Handling**

- 1 Portable Media Controls.** Contractor (including its Agents) shall only store Metro Government Information on portable device or media when expressly authorized by Metro Government to do so. When Contractor stores Metro Government Sensitive Information or on portable device or media, Contractor shall employ the following safeguards:
 - 1.1** Access to the device or media shall require a password or authentication;
 - 1.2** The device or media shall be encrypted using Strong Encryption;
 - 1.3** The workstation or portable device or media containing Metro Government Information must be clearly identified or labeled in such a way that it can be distinguished from other media or device which is not used to store Sensitive Information.
 - 1.4** The device or media must be accounted for by a system or process which tracks the movements of all devices or media which contain Metro Government Information.

- 2 Media Disposal.**
 - 2.1** Contractor shall only dispose of media containing Metro Government Information when authorized by Metro Government.
 - 2.2** Contractor shall dispose of any media which stores Metro Government Information in accordance with media sanitization guidelines for media destruction as described in the attached NIST document [NIST SP800-88: Guidelines for Media Sanitization](#).
 - 2.3** Upon Metro Government request, Contractor shall promptly provide written certification that media has been properly destroyed in accordance with this Agreement.
 - 2.4** Contractor may not transport or ship media containing Metro Government Information unless the media is Encrypted using Strong Encryption, or the information on the media has been sanitized through complete information overwrite (at least three passes); or media destruction through shredding, pulverizing, or drilling holes (e.g. breaking the hard drive platters).

- 3 Media Re-Use.**
 - 3.1** Contractor shall not donate, sell, or reallocate any media which stores Metro Government Information to any third party, unless explicitly authorized by Metro Government.
 - 3.2** Contractor shall sanitize media which stores Metro Government Information before reuse by Contractor within the Contractor facility.

SECTION ENC

Encryption and Transmission of Information

- 1** Contractor shall Encrypt Metro Government Sensitive Information whenever transmitted over the Internet or any untrusted network using Strong Encryption. Encryption of Sensitive Information within the Metro Government Network, or within Contractor's physically secured, private information center network, is optional but recommended.
- 2** Contractor shall Encrypt Metro Government Authentication Credentials while at rest or during transmission using Strong Encryption.
- 3** Contractor shall Encrypt, using Strong Encryption, all Sensitive Information that is stored in a location which is accessible from Open Networks.
- 4** If information files are to be exchanged with Contractor, Contractor shall support exchanging files in at least one of the Strongly Encrypted file formats, e.g., Encrypted ZIP File or PGP/GPG Encrypted File.
- 5** All other forms of Encryption and secure hashing must be approved by Metro Government.

SECTION IR**Incident Response**

- 1 Incident Reporting.** Contractor shall report any Information Security Incident of which it becomes aware, or failure of any technical or procedural controls, which has or had a potential to affect Metro Government Network, Metro Government Infrastructure or Metro Government Information to Metro Government and according to the following timeline and procedure:
 - 1.1** Contractor shall promptly report to Metro Government any successful Information Security Incident (with or without actual harm to system or information) within 24 hours of becoming aware of the incident. At a minimum, such report shall contain: (a) date and time when the Information Security Incident occurred; (b) the date and time when such incident was discovered by Contractor; (c) identification of the systems, programs, networks and/or Metro Government Information affected by such incident; (d) preliminary impact analysis; (e) description and the scope of the incident; and (f) any mitigation steps taken by Contractor. However, if Contractor is experiencing or has experienced a Information Breach or a successful Information Security Incident to systems that host or Store Sensitive Information or an Information Security Incident that is causing or has caused material disruption to the functionality or operation of Contractor systems or damage to Contractor hardware, software or information, including a successful attack by Malicious Software, Contractor shall report such security breach or incident to Metro Government both to the ITS Help Desk at (615) 862-HELP and to the Metro Government department within 24 hours from Contractor's reasonable awareness of such security breach or incident.
 - 1.2** Contractor shall document any attempted but unsuccessful Information Security Incident of which it becomes aware and report to Metro Government upon its request. The frequency, content, and format of such report will be mutually agreed upon by the parties.
- 2 Incident Response.**
 - 2.1** Contractor shall have a documented procedure for promptly responding to an Information Security Incidents and Information Breach that complies with applicable law and shall follow such procedure in case of an incident. Contractor shall have clear roles defined and communicated within its organization for effective internal incidence response.
 - 2.2** Contractor shall designate a contact person for Metro Government to contact in the event of an Information Security Incident. This contact person should possess the requisite authority and knowledge to: (i) act as a liaison to communicate between Contractor and Metro Government regarding the incident (including providing information requested by Metro Government); (ii) perform the reporting obligations of Contractor under this exhibit; and (iii) develop a mitigation strategy to remedy or mitigate any damage to Metro Government Network, Metro Government Infrastructure, Metro Government Information or the Product or Service provided to Metro Government that may result from the Information Security Incident.

SECTION LOG**Audit Logs**

- 1 **Audit Log Information.** The Product or Service will provide user activity Audit Log information. Audit Log entries must be generated for the following general classifications of events: login/logout (success and failure); failed attempts to access system resources (files, directories, information bases, services, etc.); system configuration changes; security profile changes (permission changes, security group membership); changes to user privileges; and actions that require administrative authority (running privileged commands, running commands as another user, starting or stopping services, etc.); . Each Audit Log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; or logical identifiers (system name, port, etc.).
- 2 **Audit Log Integrity.** Contractor shall implement and maintain controls to protect the confidentiality, availability and integrity of Audit Logs.
- 3 **User Access Audit.** Upon Metro Government’s request, Contractor shall provide Audit Logs of Metro Government’s users of the Product or Service to Metro Government.
- 4 **Audit Log Availability.**
 - 4.1 Contractor shall ensure that Audit Logs for the Product or Service for the past 90 days are readily accessible online.
 - 4.2 If for technical reasons or due to an Information Security Incident, the online Audit Logs are not accessible by Metro Government or no longer trustworthy for any reason, Contractor shall provide to Metro Government trusted Audit Log information for the past 90 days within 5 business days from Metro Government’s request.
 - 4.3 Contractor shall provide or otherwise make available to Metro Government Audit Log information which are 91 days or older within 14 business days from Metro Government’s request.
 - 4.4 Contractor shall make all archived Audit Logs available to Metro Government no later than thirty (30) days from Metro Government’s request and retrievable by Metro Government for at least one (1) year from such request.

SECTION NET**Network Security****1 Network Equipment Installation.**

- 1.1 Contractor shall not install new networking equipment on Metro Government Network without prior written permission by the Metro Government ITS department. Contractor shall not make functional changes to existing network equipment without prior written consent of such from Metro Government ITS department.
- 1.2 Contractor shall provide the Metro Government ITS department contact with documentation and a diagram of any new networking equipment installations or existing networking equipment changes within 14 days of the new installation or change.
- 1.3 Contractor shall not implement a wireless network on any Metro Government site without the prior written approval of the Metro Government ITS contact , even if the wireless network does not connect to the Metro Government Network. Metro Government may limit or dictate standards for all wireless networking used within Metro Government facility or site.

2 Network Bridging. Contractor shall ensure that no system implemented or managed by Contractor on the Metro Government Network will bridge or route network traffic.**3 Change Management.** Contractor shall maintain records of Contractor installations of, or changes to, any system on the Metro Government Network. The record should include date and time of change or installation (start and end), who made the change, nature of change and any impact that the change had or may have to the Metro Government Network, Metro Government system or Metro Government Information.**4 System / Information Access.**

- 4.1 Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.
- 4.2 Contractor shall only use Metro Government approved methods to configure Metro Government systems or application or grant access to systems.
- 4.3 Contractor shall use the Principle of Least Privilege when granting access to Metro Government Information, network or systems.

SECTION PAT**Patch Creation and Certification**

- 1 Security Patch Required.** Unless otherwise expressly agreed by Metro Government and Contractor, for Products that are no longer under performance warranty, Contractor shall provide no less than standard maintenance and support service for the Products, which service includes providing Security Patches for the Products, for as long as Metro Government is using the Products. Metro Government shall ensure that any Metro Government network that Contractor's software needs to connect to in order to provide the services are not blocked by the AV software or cause any other issues.
- 2 Timeframe for Release.** For Vulnerabilities contained within the Product that are discovered by Contractor itself or through Responsible Disclosure, Contractor shall promptly create and release a Security Patch. Contractor must release a Security Patch: (i) within 90 days for Critical Vulnerabilities, (ii) within 180 days for Important Vulnerabilities, and (iii) within one (1) year for all other Vulnerabilities after Contractor becomes aware of the Vulnerabilities. For Vulnerabilities contained within the Product that have become publicly known to exist and are exploitable, Contractor will release a Security Patch in a faster timeframe based on the risk created by the Vulnerability, which timeframe should be no longer than thirty (30) days. For the avoidance of doubt, Contractor is not responsible for creation of Security Patches for Vulnerabilities in the Product that is caused solely by the Off-the-Shelf Software installed by Metro Government.
- 3 Timeframe for Compatibility Certification.** Contractor shall promptly Certify General Compatibility of a Security Patch for third party software which the Product is dependent upon when such patch is released. For a Security Patch for Microsoft Windows Operating Systems, Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days, and shall Certify General Compatibility of an Important Security Patch within thirty (30) days, from the release of the patch. For Security Patches for Off-the-Shelf Software (OTS), Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days and Certify General Compatibility of an Important Security Patch within thirty (30) days from its release. For Security Patch for all other third party software or system, Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days and an Important Security Patch within thirty (30) days from its release. . Contractor shall publish whether the Security Patches are generally compatible with each related Product.
- 4 Notice of Un-patchable Vulnerability.** If Contractor cannot create a Security Patch for a Vulnerability, or Certify General Compatibility of a Security Patch for OTS software, within the timeframe specified herein, Contractor shall notify Metro Government of the un-patchable Vulnerability in writing. Such notice shall include sufficient technical information for Metro Government to evaluate the need for and the extent of immediate action to be taken to minimize the potential effect of the Vulnerability until a Security Patch or any other proposed fix or mitigation is received.
- 5 Vulnerability Report.** Contractor shall maintain a Vulnerability Report for all Products and Services and shall make such report available to Metro Government upon request, provided that Metro Government shall use no less than reasonable care to protect such report from unauthorized disclosure. The Vulnerability Report should (a) identify and track all known Vulnerabilities in the Products or Services on a continuing and regular basis, (b) document all Vulnerabilities that are addressed in any change made to the Product or Service, including without limitation Security Patches, upgrades, service packs, updates, new versions, and new releases of the Product or Service, (c) reference the specific Vulnerability and the corresponding change made to the Product or Service to remedy the risk, (d) specify the critical level of the Vulnerability and the applicable Security Patch, and (e) other technical information sufficient for Metro Government to evaluate the need for and the extent of its own precautionary or protective action. Contractor shall not hide or provide un-documented Security Patches in any type of change to their Product or Service.
- 6 SCCM Compatibility for Windows Based Products.** Contractor Patches for Products that operate on the Microsoft Windows Operating System must be deployable with Microsoft's System Center Configuration Manager.

SECTION REM**Remote Access to Metro Government Network/System****1 B2B VPN or Private Circuit Requirements.**

- 1.1 For Contractor's Business to Business ("B2B") or private circuit network connections which terminate on the outside of the Metro Government Network, Contractor must protect such connections by an International Computer Security Association Labs certified firewall.
- 1.2 Government may deny any traffic type due to risk and require Contractor to use a more secured protocol. Microsoft protocols such as those used in Window File Shares are considered risky and will not be allowed.
- 1.3 B2B Virtual Private Network ("VPN") connections to the Metro Government Network will only terminate on Metro Government managed network infrastructure.
- 1.4 Contractor shall authenticate the VPN to the Metro Government Network using at least a sixteen (16) character pre-shared key that is unique to the Metro Government.
- 1.5 Contractor shall secure the VPN connection using Strong Encryption.
- 1.6 Contractor shall connect to the Metro Government Network using a device capable of Site-to-Site IPSec support.
- 1.7 Contractor shall connect to the Metro Government Network using a device capable of performing policy-based Network Address Translation (NAT).
- 1.8 Contractor shall connect to the Metro Government Network through the Metro Government VPN concentrator.
- 1.9 Contractor shall not implement any form of private circuit access to the Metro Government network without prior written approval from the Metro Government ITS Department.
- 1.10 Metro Government reserves the right to install filtering or firewall devices between Contractor system and the Metro Government Network.

2 Requirements for Dial-In Modems.

- 2.1 If Contractor is using an analog line, the analog line shall remain disconnected from the modem when not in use, unless Metro Government has expressly authorized permanent connection.
- 2.2 Contractor shall provide the name of the individual(s) connecting to Metro Government Network and the purpose of the connection when requesting connectivity.

3 System / Information Access. Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.**4 Remote Access Account Usage.**

- 4.1 Upon request, Contractor shall provide Metro Government with a list of active Agent user accounts and access levels and other information sufficient for Metro Government to deactivate or disable system access if it deems appropriate.
- 4.2 Contractor may not share Metro Government-issued ID's, or any user accounts which grant access to Metro Government Network or Metro Government systems.

Exhibit A – MISA Terms and Conditions**Contract 6543886**

- 4.3** Contractor Agent shall use unique accounts assigned to the Agent to perform work. Service accounts (or accounts that are configured and used by systems to gain access to information or other systems) may not be used by Contractor Agents to access any system.

5 Metro Government Network Access Requirements.

- 5.1** Contractor shall only use Contractor systems which are compatible with Metro Government Remote Access technology to access Metro Government Network. If Contractor does not have a system that is compatible, it is Contractor's responsibility to obtain a compatible system.
- 5.2** Contractor shall implement security controls to protect Metro Government Network from risk when its systems or Agents connect to the Metro Government Network. Such controls include, but are not limited to:
- 5.2.1** Installing and maintaining ICSA Labs certified Anti-virus Software on Contractor system and, to the extent possible, use real time protection features. Contractor shall maintain the Anti-virus Software in accordance with the Anti-virus Software Contractor's recommended practices.
 - 5.2.2** Contractor may not access the Metro Government Network with systems that may allow bridging of the Metro Government Network to a non-Metro Government network.
 - 5.2.3** Contractor shall only access the Metro Government Network with systems that have the most current Security Patches installed.

6 Use of Remote Support Tools on Metro Government Network.

- 6.1** Contractor shall connect to the Metro Government Network using only Metro Government provided or approved Remote Access Software.
- 6.2** Contractor shall not install or implement any form of permanent Remote Access (e.g., GotoMyPC) on the Metro Government Network or Metro Government systems.

7 Remote Control Software

- 7.1** Contractor may not install any form of Remote Control Software on systems that are maintained or administered by Metro Government without Metro Government's consent. Contractor is only allowed to install Remote Control Software on Contractor Managed Systems.
- 7.2** Remote Control Software must secure all network traffic using Strong Encryption.
- 7.3** Contractor shall ensure that Remote Control Software contained within the Product supports the logging of session establishment, termination, and failed login attempts. Each log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; and network identifiers (IP address, MAC Address, etc.) or logical identifiers (System name, port, etc.). For Contractor Maintained Systems, Contractor shall ensure that such systems are configured to do the above.
- 7.4** Remote Control Software shall not provide escalation of user account privileges.
- 7.5** Contractor shall only access the Metro Government Network via Metro Government approved remote access methods. Contractor shall not supply Products, nor make configuration changes that introduce non-approved forms of Remote Access into the Metro Government Network.

SECTION SOFT**Software / System Capability****1 Supported Product.**

- 1.1 Unless otherwise expressly agreed by Metro Government in writing, Contractor shall provide Metro Government only supported versions of the Product, which will not become "end of life" for at least 24 months. When the Product or Service requires third party components, Contractor must provide a Product that is compatible with currently supported third party components. Unless otherwise expressly agreed by Metro Government, Contractor represents that all third party components in its Product are currently supported, are not considered "end of life" by the third party provider of such components, and will not become "end of life" in less than 24 months from the date of acquisition by Metro Government.
- 1.2 If Open Source Software is incorporated into the Product, Contractor shall only use widely supported and active Open Source Software in the Product, and shall disclose such software to Metro Government prior to its acquisition of the Product.
- 1.3 Information transfers within applications and involving services should be done using web services, APIs, etc. as opposed to flat file information transport.

2 Software Capabilities Requirements.

- 2.1 Contractor shall disclose to Metro Government all default accounts included in their Product or provide a means for Metro Government to determine all accounts included in the Product.
- 2.2 Contractor shall not include fixed account passwords in the Product that cannot be changed by Metro Government. Contractor shall allow for any account to be renamed or disabled by Metro Government.
- 2.3 Contractor's Product shall support a configurable Session Timeout for all users or administrative access to the Product.
- 2.4 Contractor shall ensure that the Product shall transmit and store Authentication Credentials using Strong Encryption.
- 2.5 Contractor Products shall mask or hide the password entered during Interactive User Login.
- 2.6 Contractor shall ensure that Products provided can be configured to require a Strong Password for user authentication.
- 2.7 Contractor's Product shall allow user accounts to be disabled after a configurable amount of failed login attempts over a configurable amount of time.
- 2.8 Contractor's Product shall have the capability to require users to change an initial or temporary password on first login.
- 2.9 Contractor's Product shall have the capability to report to Metro Government, on request, all user accounts and their respective access rights within three (3) business days or less of the request.
- 2.10 Contractor's Product shall have the capability to function within Metro Governments Information Technology Environment. Specifications of this environment are available upon request.

- 3 **Backdoor Software.** Contractor shall not provide Products with Backdoor Software, including, without limitation, undocumented or secret access functions (e.g., accounts, authorization levels, over-rides or any backdoor). Contractor shall supply all information needed for the Metro Government to manage all access (local or remote) capabilities within the Product including denying of Remote Access entirely from any party including Contractor. Contractor shall not include any feature within the Product that would allow anyone to circumvent configured authorization remotely.

SECTION VMGT**Contractor Managed System Requirements****1 Vulnerability and Patch Management.**

- 1.1 For all Contractor Managed Systems that store Metro Government Information, Contractor will promptly address Vulnerabilities through Security Patches. Unless otherwise requested by Metro Government, Security Patches shall be applied within fourteen (14) days from its release for Critical Security Patches, thirty (30) days for Important Security Patches, and twelve (12) months for all other applicable Security Patches. Contractor may provide an effective technical mitigation in place of a Security Patch (if no Security Patch is available or if the Security Patch is incompatible) which doesn't materially impact Metro Government's use of the system nor require additional third party products.
- 1.2 If the application of Security Patches or other technical mitigations could impact the operation of Contractor Managed System, Contractor agrees to install patches only during Metro Government approved scheduled maintenance hours, or another time period agreed by Metro Government.
- 1.3 Contractor Managed Systems on the Metro Government Network or Metro Government Infrastructure, the Metro Government retains the right to delay patching for whatever reason it deems necessary.
- 1.4 Metro Government will monitor compliance and check for Vulnerabilities on all Products on the Metro Government Network or Metro Government Infrastructure. Contractor shall provide Metro Government administrative credentials upon request for the purpose of monitoring compliance of a given Product. Metro Government will not knowingly change configurations of the Contractor Managed Systems without prior approval from Contractor.
- 1.5 Government may monitor compliance of Contractor Managed Systems. Contractor agrees to allow Metro Government to check for Vulnerabilities during agreed upon times using mutually agreed upon audit methods.
- 1.6 Contractor shall use all reasonable methods to mitigate or remedy a known Vulnerability in the Contractor Managed System according to the level of criticality and shall cooperate fully with Metro Government in its effort to mitigate or remedy the same. Upon Metro Government's request, Contractor shall implement any reasonable measure recommended by Metro Government in connection with Contractor's mitigation effort.

2 System Hardening.

- 2.1 Contractor Managed Systems, Contractor shall ensure that either: (i) file shares are configured with access rights which prevent unauthorized access or (ii) Contractor shall remove or disable file shares that cannot be configured with access controls set forth in (i) hereof. Access rights to file shares that remain under (i) must use the Principle of Least Privilege for granting access.
- 2.2 In the event that Contractor is providing Products or systems that are to be directly accessible from the Internet, Contractor shall disable or allow disabling by Metro Government of all active or executed software components of the Product or system that are not required for proper functionality of the Product or system.
- 2.3 Contractor shall ensure that Contractor Managed Systems are synchronized with reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC). In the case of systems residing on the Metro Government Network, Contractor shall ensure that all such systems are synchronized with an Metro Government corporate timeserver in their respective Regional Information Centers (RDC).
- 2.4 For Contractor Managed Systems, Contractor shall remove or disable any default or guest user accounts. Default accounts that cannot be removed or disabled must have their default password changed to a Strong Password that is unique to the respective site and Metro Government.
- 2.5 For Contractor Managed Systems, Contractor shall ensure that the system is configured to disable user accounts after a certain number of failed login attempts have occurred in a period of time less than thirty (30) minutes of the last login attempt or that system monitoring and notification is configured to alert system administrators to successive failed login attempts for the same user account.

Exhibit A – MISA Terms and Conditions**Contract 6543886****3 Authentication.**

- 3.1 Contractor shall assign a unique user ID to any Agent or end user who accesses Sensitive Information on Contractor Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.
- 3.2 Contractor agrees to require authentication for access to Sensitive Information on Contractor Managed System.
- 3.3 Contractor agrees to configure the system to support Strong Authentication for accessing Sensitive Information from any Open Network (e.g., Internet, open wireless). For avoidance of doubt, Metro Government Network is considered a trusted network.
- 3.4 Contractor shall configure the system to expire passwords at least every one-hundred and eighty (180) days and require a password change on the next successful login. For system that cannot support Strong Passwords, Contractor shall configure the system to expire passwords every ninety (90) days.
- 3.5 Unless otherwise agreed by Metro Government, Contractor shall ensure that Contractor Managed Systems will require Strong Password for user authentication.

4 **Automatic Log off.** Contractor shall configure systems which store Sensitive Information to automatically logoff user sessions at the most after 20 minutes of inactivity.

5 **User Accountability.** Contractor shall report to Metro Government, on request, all user accounts and their respective access rights within the system within five (5) business days or less of the request.

6 **Information Segregation, Information Protection and Authorization.** Contractor shall implement processes and/or controls to prevent the accidental disclosure of Metro Government Sensitive Information to other Contractor Metro Governments, including an Affiliates of Metro Government.

7 **Account Termination.** Contractor shall disable user accounts of Agents or Metro Government end users for the system within five (5) business days of becoming aware of the termination of such individual. In the cases of cause for termination, Contractor will disable such user accounts as soon as administratively possible.

8 System / Information Access.

- 8.1 Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.
- 8.2 Contractor agrees to use the Principle of Least Privilege when granting access to Contractor Managed Systems or Metro Government Information.

9 System Maintenance.

- 9.1 Contractor shall maintain system(s) that generate, store, transmit or process Metro Government Sensitive Information according to manufacturer recommendations. Contractor shall ensure that only those personnel certified to repair such systems are allowed to provide maintenance services.
- 9.2 Contractor shall keep records of all preventative and corrective maintenance on systems that generate, store, transmit or process Metro Government Sensitive Information. Such records shall include the specific maintenance performed, date of maintenance, systems that the maintenance was performed on including identifiers (e.g., DNS name, IP address) and results of the maintenance. Upon request by Metro Government, Contractor shall supply such record within thirty (30) days.

NIST SP800-88: Guidelines for Media Sanitization**ITL BULLETIN FOR FEBRUARY 2015****NIST SPECIAL PUBLICATION 800-88 REVISION 1,
GUIDELINES FOR MEDIA SANITIZATION**

Andrew Regenscheid, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

NIST has published an updated version of [Special Publication \(SP\) 800-88, Guidelines for Media Sanitization](#). SP 800-88 Revision 1 provides guidance to assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information. Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. Information disposition and sanitization decisions occur throughout the information system life cycle.

The publication states that the types of media used to create, capture, or transfer information used by the system should be determined during the requirements phase of the system. This analysis, balancing business needs and risk to confidentiality, will formalize the media that will be considered for the system to conform to Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.

Media sanitization is one of the key elements in assuring confidentiality. In order for organizations to have appropriate controls of the information they are responsible for safeguarding, they must properly secure used media.

SP 800-88 Revision 1 recommends processes to guide media sanitization decision making regardless of the type of media in use. To effectively use this guide, organizations and individuals should focus on the information that may have been stored on the media, rather than focusing on the media itself. The document also includes guidelines and recommendations on methods for sanitizing different types of media, as described below.

Types of Sanitization

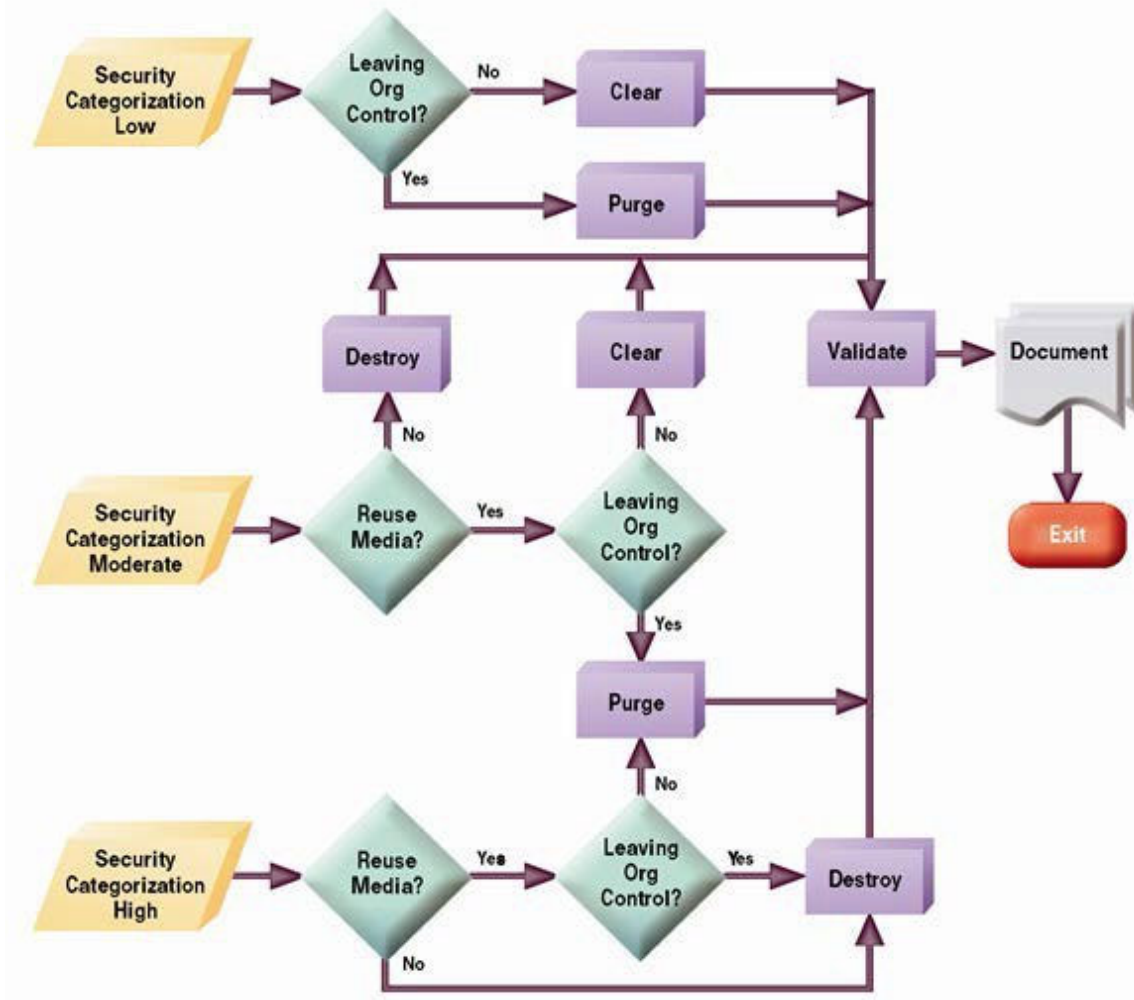
The publication describes three types of media sanitization – Clear, Purge, and Destroy - that can help ensure that data is not unintentionally released. These types are defined as follows:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple noninvasive data recovery techniques; it is typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

- **Purge** applies physical or logical techniques that render target data recovery infeasible using state-of-the-art laboratory techniques.
- **Destroy** renders target data recovery (using state-of-the-art laboratory techniques) infeasible and results in the subsequent inability to use the media for storage of data.

Sanitization methods for specific media/device types are provided in Appendix A of the document.

Organizations using this guide should categorize the information to be protected, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, the organization can choose the appropriate type(s) of sanitization. The **chart below** provides a decision process flow to assist organizations in making sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media. This decision process is based on the confidentiality of the information, not the type of media. Once organizations decide what type of sanitization is best for their individual case, then the media type will influence the technique used to achieve this sanitization goal.



Verification Methods

The publication recommends two types of sanitization verification. The first is to perform verification every time sanitization is applied. The second is a representative sampling verification, applied to a selected subset of the media. If possible, the sampling should be executed by personnel who were not part of the original sanitization action. The goal of sanitization verification is to ensure that the target data was effectively sanitized. SP 800-88 Revision 1 provides different methods of verification based on destructive techniques that have been used.

Trends in Data Storage Media

SP 800-88 Revision 1 provides analysis of trends in growing storage capacity and describes revolutionary and evolutionary changes in sanitization. The publication mentions that media technologies, such as flash memory-based storage devices including Solid State Drives (SSDs) and self-encrypting drives, have become prevalent. Degaussing and overwriting techniques - common methods for sanitizing magnetic media - are not applicable for flash memory devices. Evolutionary changes in magnetic media also have impacts on sanitization. New storage technologies, and even variations of magnetic storage, are dramatically different from legacy magnetic media. These clearly require sanitization research and a reinvestigation of sanitization procedures to ensure efficacy.

Trends in Sanitization

The publication summarizes some trends in sanitization. For storage devices containing *magnetic* media, a single overwrite pass with a fixed pattern, such as binary zeros, typically hinders recovery of data even if state-of-the-art laboratory techniques are applied to attempt to retrieve the data. One major drawback of relying solely upon the native Read and Write interface for performing the overwrite procedure is that areas that are not currently mapped to active areas (e.g., defect areas, over provisioned, unallocated space) may not be securely sanitized. These native methods also may not reliably overwrite all areas when wear-leveling techniques (commonly used with flash memory) are employed. Dedicated sanitization commands may support addressing these areas more effectively, but also require a level of assurance from the vendor.

Destructive techniques for some media types may become more difficult or impossible to apply in the future. Traditional techniques such as degaussing (for magnetic media) become more complicated as magnetic media evolves, because some emerging variations of magnetic recording technologies incorporate media with higher coercivity (magnetic force). As a result, existing degaussers may not have sufficient force to effectively degauss such media.

Cryptographic Erase (CE) is an emerging sanitization technique that can be used in some situations when data is encrypted as it is stored. With CE, media sanitization is performed by erasing the cryptographic keys that were used to encrypt the stored data, as opposed to sanitizing the storage locations on media containing the encrypted data itself. However, operational use of CE today presents some challenges. In some cases, it may be difficult to verify that CE has effectively sanitized media. SP 800-88 Revision 1 describes this challenge and possible approaches.

Conclusion

Both revolutionary and evolutionary changes make sanitization decisions more challenging, as the storage device may not clearly indicate what type of media is used for data storage. The burden falls on the user to accurately determine the media type and apply the appropriate sanitization procedure. SP 800-88 Revision 1 will assist organizations and system owners in making sanitization decisions. It does not, and cannot, specifically address all known types of media; however, the described sanitization decision process can be applied broadly.

ITL Bulletin Publisher: Elizabeth B. Lennon Information Technology
Laboratory
National Institute of Standards and Technology elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

Proprietary Notice



The information disclosed in this document, including all designs and related materials, is the valuable property of NEC Corporation of America, (hereinafter "NEC") and/or its licensors. NEC and/or its licensors, as appropriate, reserve all patent, copyright, and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

You may not remove, overprint, or deface any notice of copyright, trademark, logo, legend, or other notice of NEC ownership from any originals or duplicates of any software or hardware products of NEC disclosed in this document. The names, logos, copyrights, trademarks, and service marks of NEC appearing in this document may not be used in any advertising or publicity or otherwise to indicate sponsorship of or affiliation with any product or service, without NEC's express prior written permission.

The NEC product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product or a separate written warranty agreement that may be applicable. However, actual performance of each such product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by NEC.

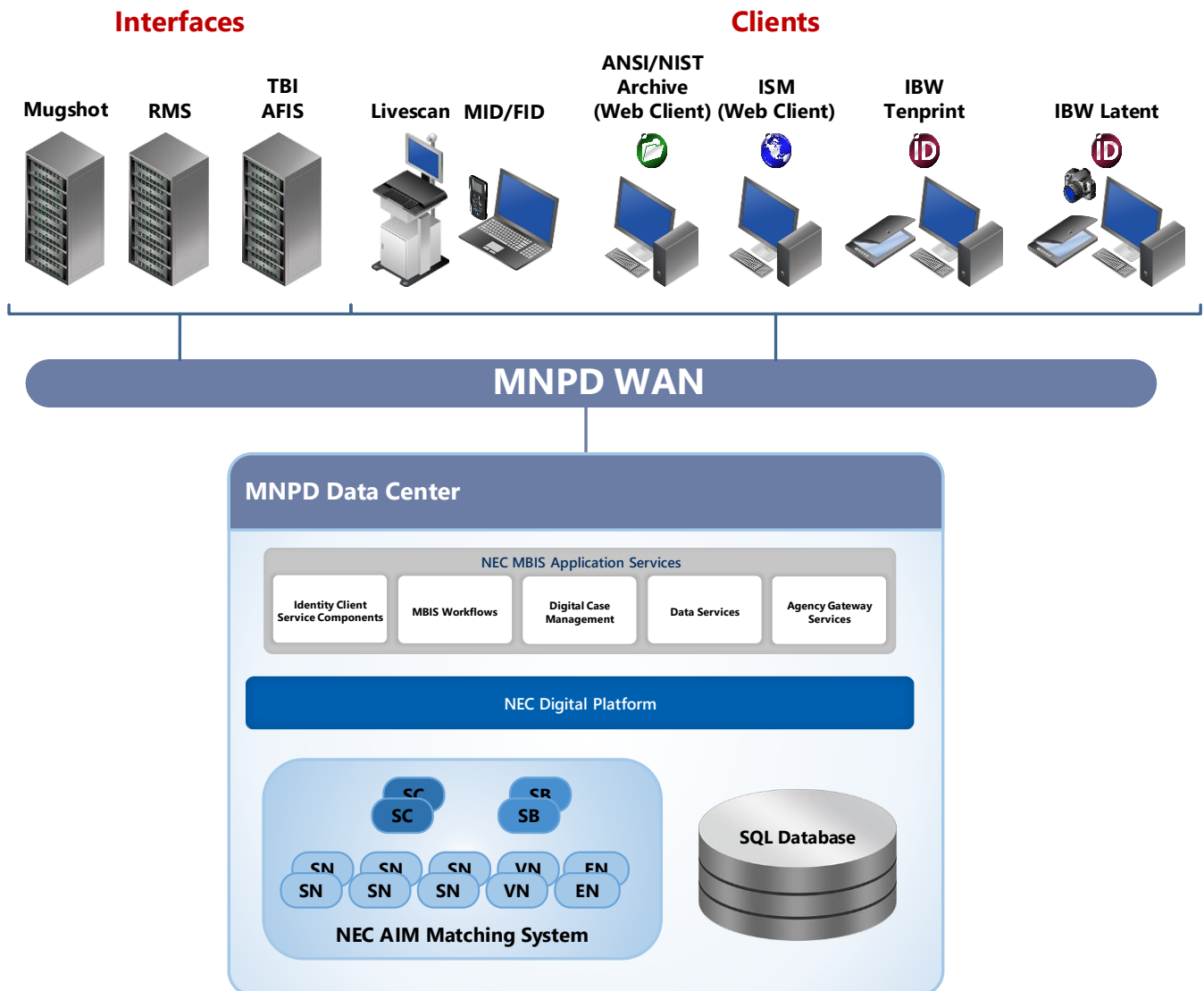
To allow for design and specification improvements, the information in this document, and the products and services described in such information, are subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of NEC is prohibited.

Copyright © 2024 NEC Corporation of America

1 Project Overview

NEC will build and deliver an on-premise system as outlined in this SOW. The Integra-ID architecture focuses on the integration of proven hardware and software to provide a solid infrastructure that can fully support all of Metropolitan Nashville Police Departments’ (MNP) identification requirements. Figure 1 provides a high-level diagram illustrating the Integra-ID system.

Figure 1: Integra-ID MIBS Configuration



1.1 Components

Table 1 describes the NEC-provided base system components of the solution.

Table 1: Components

System Components	Description
NEC Digital Platform (NDP) Transaction Controller Server	The NDP manages all workflows and all external interfaces. It maintains the work-in-progress (WIP) queue and tracks all activities and roles for all users. The NDP hosts all the necessary external interfaces, workstation interfaces, administrative access, and online reporting. The NDP houses all MBIS transaction control and Archive services and provides a centralized location for logging and auditing data. .
Image Processing Controller (IPC)	Used for feature extraction, automatic classification, finger sequence check, and quality control, the IPC processes fingerprint and palmpint images.
Unified Database (UDB)	The UDB manages all access to the system and stores MBIS images, descriptive information, feature data, necessary audit trail data, report data, user profile data, and, for the NIST Archive metadata search component, the original NIST records and associated metadata.
AIM X ^M Multimodal Matcher	<p>AIM X^M provides integrated services for fingerprint and palmpint matching with the following key components:</p> <ul style="list-style-type: none"> • Search Controller (SC) – Manages the feature container storage and the loads on the search brokers. It also manages the gallery segmentation to the search nodes. • Search Broker (SB) – Manages the requests and workload on the search extract and verify nodes. It distributes jobs and aggregates responses. • Search Node (SN) – Performs one-to-many (1:N) searching. It communicates with other search nodes using peer to peer SLA management to distribute gallery segments when necessary. • Extract Node (EN) – Assesses the image quality of submitted images and encodes images to feature data for matching. • Verify Node (VN) – Performs one-to-one (1:1) verification matching.
Integrated Biometric Workstation (IBW)	IBW, a Microsoft Windows-based PC software suite, serves as the user interface to the Integra-ID MBIS. It provides a single logon point to run all available user functions, including all tenprint, latent and palmpint functionality. User profile and workstation purpose, however, dictate available functions.

System Components	Description
	<p>These workstations provide the feature rich user experience of a client-server model. Using Windows 10’s enhanced touchscreen capabilities, IBW provides a contemporary and interactive user interface while also providing support for keyboard and mouse user interfaces.</p>
FastID Workstation	<p>The FastID workstation provides a 1:1 and 1:N fingerprint identification function for the non-fingerprint expert. It is a lights-out process used for pre-booking and jail management identification needs.</p> <p>Each workstation will have a single-finger scanner.</p> <p>Built using the .NET platform, these workstations provide the feature rich user experience of a client-server model.</p>
SmartScan Livescan	<p>NEC has transformed livescan biometric technology with SmartScan, a sleek, scalable, secure, and easy to operate solution that manages forensic-grade fingerprint (rolled and slap), palmprint (full, split, and writer’s), and face images collection, with support for future modalities, such as scars/marks/tattoos (SMT) and iris images. For fixed locations, SmartScan can be housed in NEC’s UnCabinet, which provides a better alternative to capturing these multimodal biometric images.</p>

1.2 Design Parameters

NEC will provide the following baseline design parameters:

Table 2: Database Parameters

Database	Conversion	Design	Remarks
Subjects	858,000	1,500,000	
Rolled Database – Tenprint (RDB-T)	858,000	1,500,000	20-Finger database for Tenprint
Slap Database – Tenprint (SDB-T)	860,000	1,500,000	
Rolled Database – Latent Search (RDB-L)	860,000	2,000,000	20-Finger database for Latent
Slap Database – Latent Search (SDB-L)			
Latent Fingerprint Database (LDB)	60,000	75,000	
Palmprint Database – Full (PDB)	995,000	1,500,000	

Database	Conversion	Design	Remarks
Latent Palmprint Database (LDB-P)	5,500	15,000	
NIST Archive	1,860,000	2,500,000	

Table 3: Transaction Volumes

Transaction Volumes	Daily	Peak	Avg. Response Time (Seconds)	Op. Hours	Remarks
Tenprint Submission	350	100		24	
Tenprint Inquiry (TI)	350	100	60	24	
Latent Inquiry (LI) Fusion (RDB-L and SDB-L)	80	25	300	24	
Tenprint-to-Latent Inquiry (TLI)	350	100	300	24	
Latent-to-Latent Inquiry (LLI)	40	12	300	24	
FastID Searches 1:N	350	100	30	24	
Palmprint Submission	350	100		24	
Palmprint-to-Latent Palmprint Inquiry (TLI-P)	35	100	300	24	
Latent Palmprint-to-Full Palmprint Inquiry (LI-P)	50	10	300	24	
Latent Palmprint-to-Latent Palmprint (LLI-P)	25	5	300	24	

1.3 Workflow Overview

Figure and 3 provides an overview of MNPD’s Automated booking workflow. This workflow is implemented on the existing system.

Figure 2: Automated Booking Workflow Overview

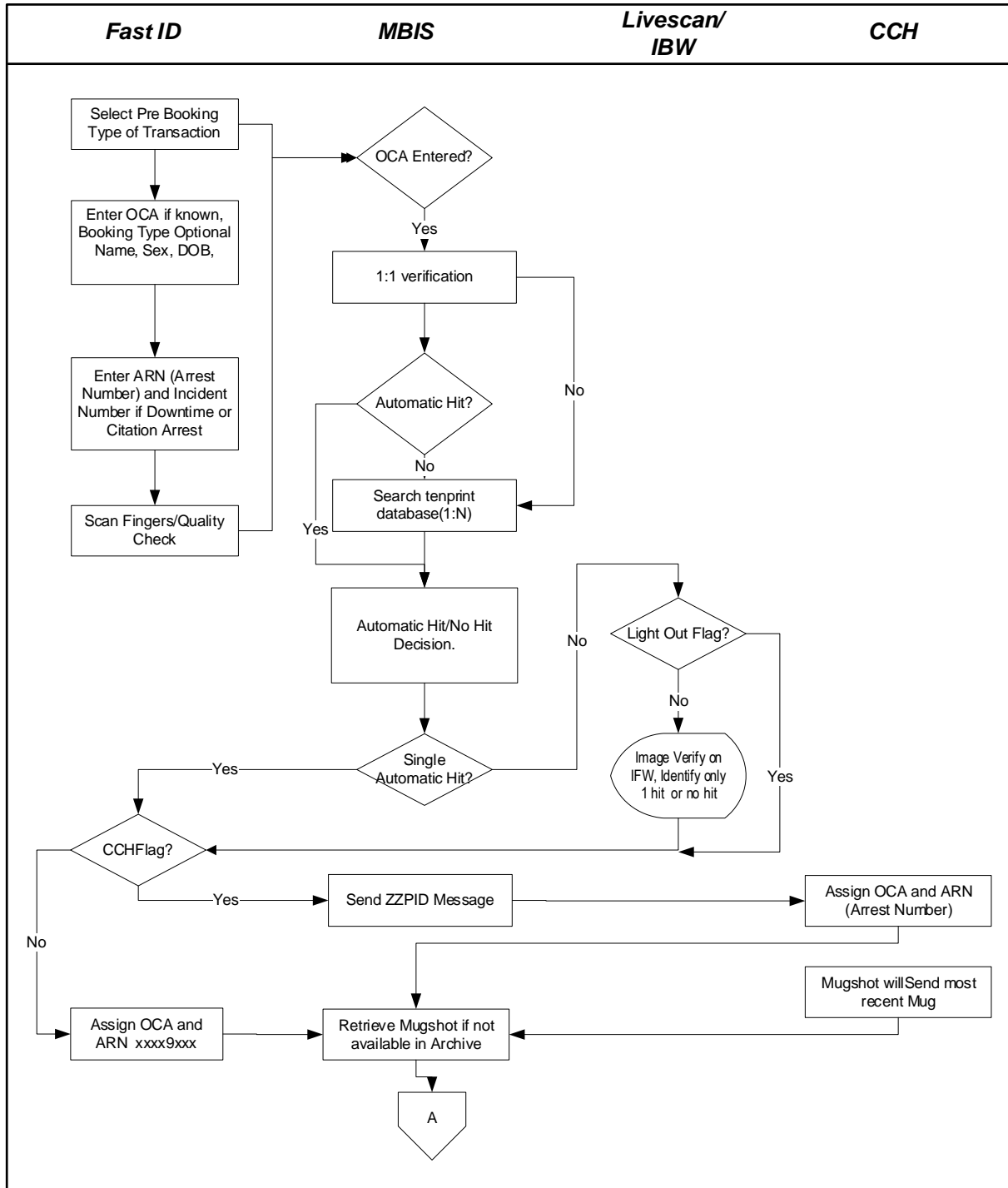


Figure 3: Automated Booking Workflow Overview (Cont.)

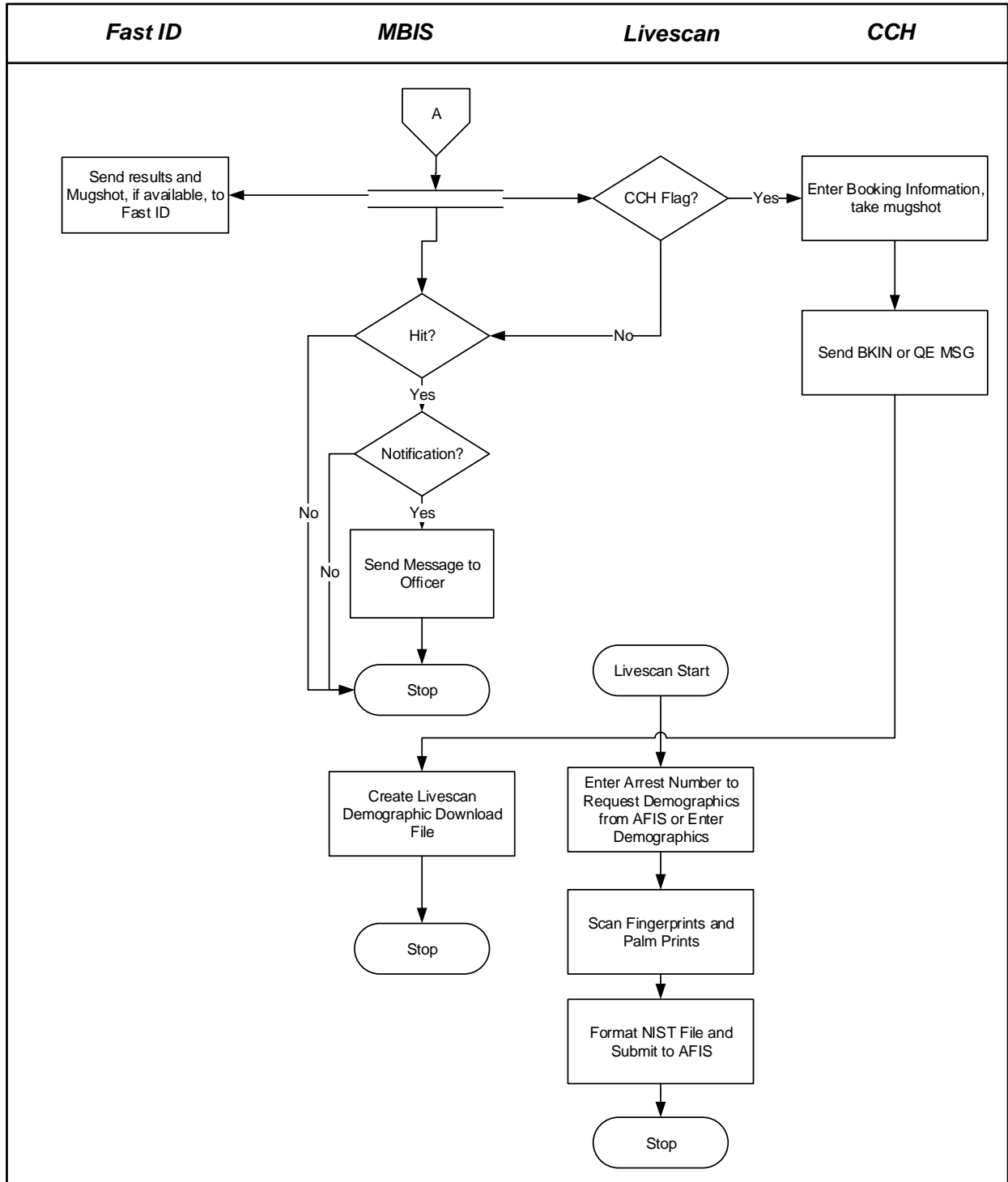


Figure 4: Manual Tenprint Workflow Overview

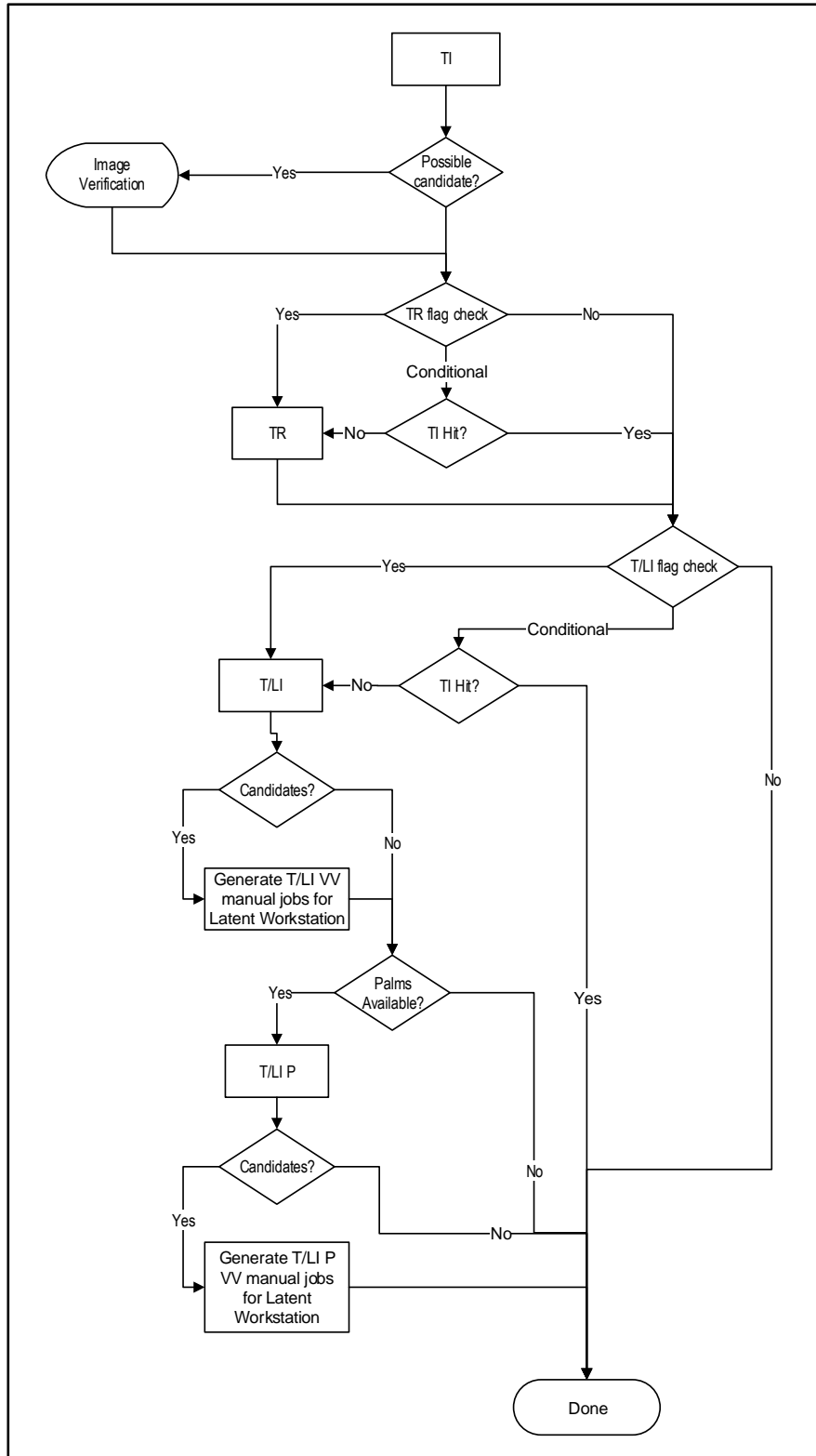


Figure 5 provides an overview of the latent workflow.

Figure 5: Latent Workflow Overview

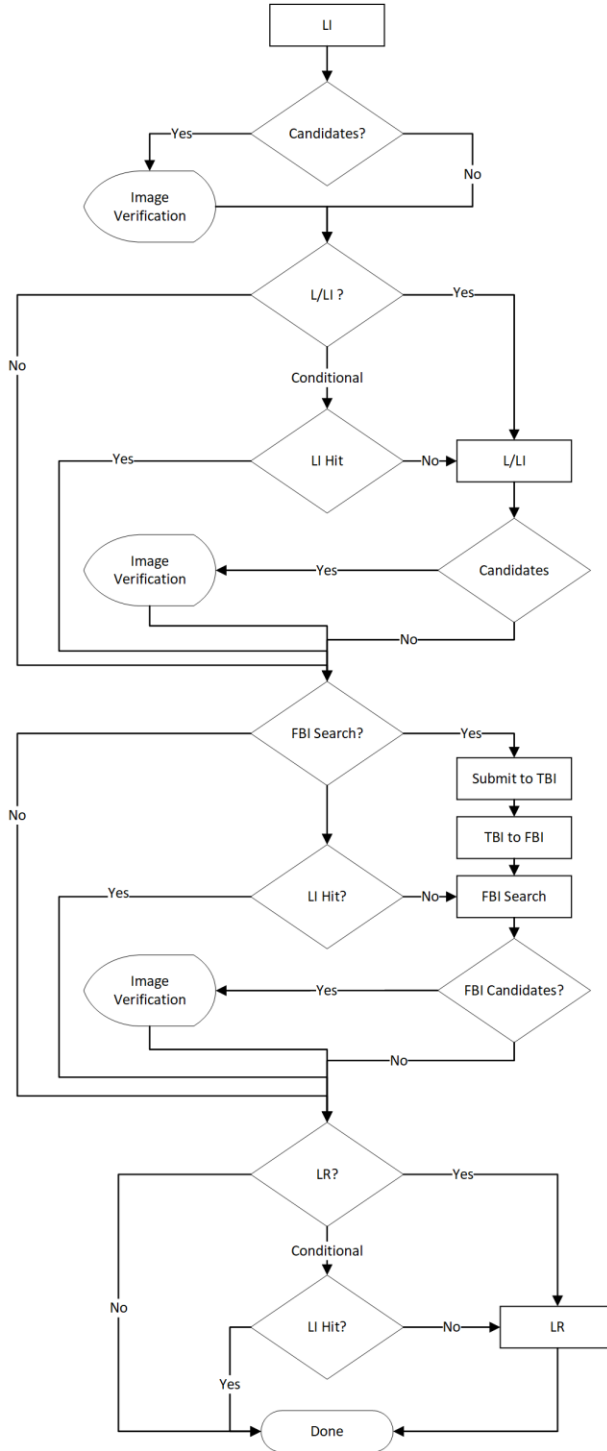
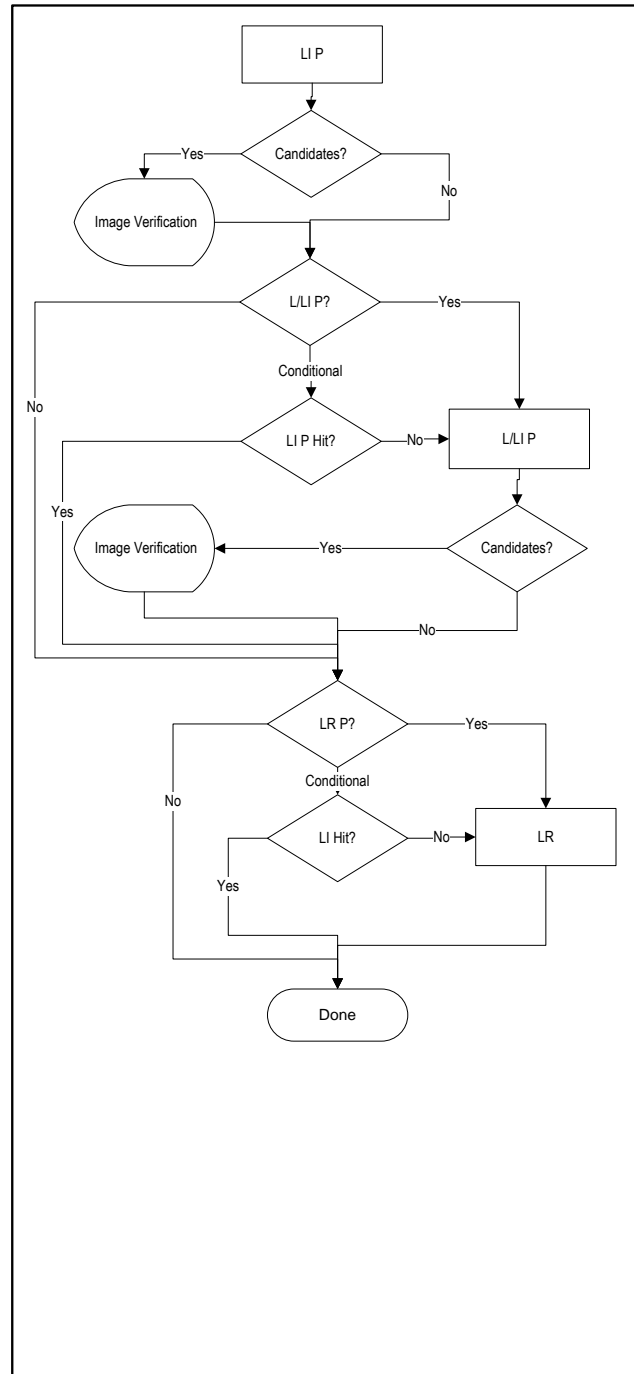


Figure 6 provides an overview of the latent palm workflow.

Figure 6: Latent Palm Workflow Overview



1.4 Project Deliverables and Services

NEC’s is providing a turnkey solution designed to meet Metropolitan Nashville Police Department’s needs and specifications. Table 4: Table 4 is an overview of the project deliverables and services NEC is providing.

Table 4: Project Deliverables and Services

Scope	Deliverables
Integra-ID	<ul style="list-style-type: none"> • Integra-ID Platform including: <ul style="list-style-type: none"> ▪ NDPTtransaction Controller ▪ Image Processing Controller ▪ Unified Database (with a design capacity as described in Section 1.2) ▪ AIM XM search controller, search broker, search nodes, extract nodes, and verification nodes to meet requirements stated in Section 1.2 • (5) IBW Tenprint workstations (Tenprint, Verification) <ul style="list-style-type: none"> ▪ NEC will provide the following: <ul style="list-style-type: none"> ○ (5) IBW Tenprint workstation licenses ▪ MNPD will provide the following: <ul style="list-style-type: none"> ○ (5) Desktop PCs ○ (8) Monitors ○ (5) Epson V850 Flatbed Scanners • (12) IBW Latent Workstations <ul style="list-style-type: none"> ▪ NEC will provide the following: ▪ (12) IBW Latent workstation licensesMNPD will provide the following: <ul style="list-style-type: none"> ○ (12) Desktop PCs ○ All Monitors ○ (2) Epson V850 Flatbed Scanners • (6) FastID workstations <ul style="list-style-type: none"> ▪ NEC will provide the following:* <ul style="list-style-type: none"> ○ (6) FastID workstation licenses ○ (6) Watson Mini Single Finger Scanners ▪ MNPD will provide the following: <ul style="list-style-type: none"> ○ (6) Desktop Optiplex PCs ○ (6) Dell 20-inch monitors • (6) Network B&W Lexmark MS821dn Printers* • (5) FBI Certified Card Printers (Lexmark MS821dn)* • (7) SmartScan kiosk

Scope	Deliverables
	<ul style="list-style-type: none"> ▪ NEC will provide the following:* <ul style="list-style-type: none"> ○ (7) SmartScan licenses ○ (7) NEC ruggedized Uncabinets ○ (7) Dell Optiplex micro-PC and 21-inch monitors ○ (7) 500 ppi Thales CS500Q finger and palm scanners* • (2) SmartScan desktop workstations <ul style="list-style-type: none"> ▪ NEC will provide the following:* <ul style="list-style-type: none"> ○ (2) SmartScan licenses ○ (2) Dell Optiplex mico-PCs and 21-inch single touch monitors ○ (2) 500 ppi Thales CS500Q finger and palm scanners* • (10) Archive Web Client Licenses • (3) High Volume Scanning Workstations with High Volume Scanners <ul style="list-style-type: none"> ▪ NEC will provide the following:* <ul style="list-style-type: none"> ○ (3) High Volume Scanning licenses ○ (3) Fujitsu FI-7600 Scanners ▪ MNPD will provide the following: <ul style="list-style-type: none"> ○ (3) Dell Optiplex PCs and Dell 21-inch single monitor • (1,000) NDP Mobile-ID Client Device Licenses
Development of Interfaces	<ul style="list-style-type: none"> • Livescan interface • RMS interface • TBI interface (tenprint submissions and responses) • Mugshots (for Fast-ID and Archive) • FBI interface for latent submissions (through TBI) • Mobile-ID interface
Workflow Design and Configuration	<ul style="list-style-type: none"> • Tenprint workflow as defined in Section 1.3 • Latent Workflow as defined in Section 1.3 • Latent Palm Workflow as defined in Section 1.3
Implementation Services	Defined in Section 1.4.1
1-Year Warranty	<ul style="list-style-type: none"> • 24 x 7 coverage after system acceptance • 8 x 5 onsite engineer **
Maintenance Services	<ul style="list-style-type: none"> • 24 x 7 coverage after warranty period • 8 x 5 onsite engineer** • VPN/remote support to provide first- and second-level support as required • Local spare parts inventory of critical components • Annual joint technology review during which NEC will share product MBIS technology product roadmap

Scope	Deliverables

*Due to ongoing supply chain issues, NEC may need to substitute items of equipment and software (“Substitutions”), provided that such substitution will not adversely affect the functionality and performance of the deliverables. Substitutions do not adjust a fixed priced contract. NEC will provide written notification of such changes.

**Onsite Engineer may work remotely from home office, but must be able to respond onsite within 2 hours.

1.4.1 Project Management

The NEC Project Management Organization (PMO) and its certified Project Management Professionals (PMP) have defined a project lifecycle methodology that closely aligns to the current Project Management Body of Knowledge (PMBOK) standards from the Project Management Institute (PMI). The NEC Project Manager will use best practices that are agile and measurable to ensure a quality implementation and provide a comprehensive interface with the Client throughout the Project.

The following section summarizes the standard implementation activities for each of the major project phases.

1.4.1.1 Planning

- Conduct Initial Kickoff Meeting
- Update Project Management Plan (PMP) and Integrated Master Schedule (IMS) and submit to Client for review
- Update PMP and IMS per Client input
- Obtain Client approval

1.4.1.2 System Requirements

- Analyze and document Client requirements in Business Requirements Document (BRD)
- Conduct Site Survey
- Incorporate Survey Results into BRD
- Prepare Agenda/Presentation Materials for Business Requirement Review (BRR)
- Submit BRD and Meeting Documentation for Client’s review
- Conduct BRR and update BRD based on BRR
- Resubmit BRD and obtain Client approval

1.4.1.3 System Design

- Create and submit the following design documents for Client's review
 - Interface Requirements Document (IRD)
 - Equipment List
 - Installation Plan
 - Training Plan
- Prepare Agenda/Presentation Materials for System Design Review (SDR)
- Submit design documents and Meeting Documents to Clients for review
- Conduct SDR and update design documents based on SDR
- Re-submit design documents and obtain Client approval

1.4.1.4 System Configuration

- Create conversion tool
- Create database schema and script development for conversion
- Configure workflows
- Configure the following interfaces:
 - Livescan interface
 - Archive interface
 - RMS interface
 - TBI interface (tenprint submissions and responses)
 - Mugshots (for Fast-ID and Archive)
 - FBI interface for latent submissions
 - Mobile-ID interface
- Configure and customize the Transaction Controller components
- Configure and customize the IBW components
- Configure and customize the SmartScan components
- Configure and customize the FastID components
- Configure and customize the Reporting components

1.4.1.5 Testing

- Conduct system testing including:
 - Conversion Tool Testing
 - Perform Testing of workflows, interfaces, Transaction Controller, IBW, Reporting, SmartScan, and FastID

1.4.1.6 Production Environment Deployment and Testing

- Procure materials
- Receive hardware and software
- Deploy system configuration
- Setup and configure production hardware
- Test production system

1.4.1.7 Factory Acceptance Testing

- Prepare FAT documentation including:
 - FAT Plan
 - FAT Procedures
- Conduct FAT at NEC facility
- MNPD personnel will participate remotely through videoconferencing

1.4.1.8 Data Migration

- Analyze the existing system to identify various data categories and different types of data (NIST types, Image types etc)
- Collect samples of different datasets
- Identify the New Tools / Tool modifications needed
- Develop/Modify Data Migration Tools
- Test the Data Migration Tools with sample data
- Prepare the Data Migration environment/configure the tools
- Process various categories of data
- Validate migrated data
- Analyze the exceptions and apply fixes
- Process Incremental Catchups
- Final reconciliation and reporting

1.4.1.9 Installation

- Ship onsite components to Client's facilities
- Perform hardware installation
- Installation Test – SAT rehearsal

1.4.1.10 System Acceptance Test

- Prepare SAT documentation including:

- SAT Plan
- SAT Procedures
- Conduct SAT at Client site

1.4.1.11 Training and Documentation

- Conduct Tenprint training
- Conduct Latent training
- Conduct Fast-ID training
- Conduct Archive training
- Conduct SmartScan training
- Conduct Mobile-ID train-the-trainer training
- Conduct training for managers and supervisors
- Integrated online help user documentation

1.4.1.12 Conduct Switchover

- Commission and test system
- System switches over to production

1.4.1.13 Administrative Closing

- Transition to Operations
- Administratively close project

1.5 Client Responsibilities

- Provide wide area network (WAN) and local area network (LAN) infrastructure for the Integra-ID system.
- CJIS Security compliance including:
 - Advanced authentication
 - Encryption of Criminal Justice Information (CJI) on the mobile device
 - Encryption of CJI in communication
- Network TCP/IP address and any network enhancements to provide access to Integra-ID
- Integration testing of all existing livescan systems that submit to Client, if applicable
- Provide system(s) interface specifications, external modifications, and testing with the Integra-ID interface
- Supply and install anti-virus software
- Management and maintenance of any non-NEC software according to their respective manufacturer specifications, including antivirus and OS maintenance and updates.

- Both NEC and client will work to prevent project delays. If there were unbudgeted costs to NEC, and the cause of the delays are agreed to be solely due to client, then the client and NEC will work together to identify and agree on the payment for unbudgeted costs.

1.6 Bandwidth Requirements

NEC’s standard recommended bandwidth requirements are provided in the following tables.

Central Site Product Type	500ppi	1000ppi
Biometric Workstation (Latent, Tenprint, Palm)	100 Mb Fast Ethernet	1Gb Ethernet
Inter-AFIS server communication**	1Gb Ethernet	1Gb Ethernet
Central Site Remote Connection (inbound/outbound traffic to remotes)	10 Mb	25 Mb

*Archive usage is based upon average document sizes of 700kb.

**Inter-AFIS server networking is provided by NEC; all other networking costs are the responsibility of the customer.

2 Definitions

Capitalized terms not otherwise defined in this SOW or the Agreement have the following meanings:

Table 5: Components

Term	Definition
Deliverables	The Equipment and Services plus any other tangible items (e.g., reports, project plans, checklists, etc.) to be provided to Client as specified in this SOW.
Equipment	Both hardware products and software sold, licensed, or installed as specified in this SOW.
Project Completion	That point in the Project when NEC has completed the Services and provided the Deliverables to Client.
Services	The installation, maintenance, professional, or other related Services as specified in this SOW.

Term	Definition
Software	The machine-readable object code software programs, if any, licensed by NEC or its suppliers as specified in this SOW.

3 Project Schedule

NEC will confer with Client after the Effective Date of this SOW, to define a Project schedule. The Project schedule will include, but will not be limited to, the Project commencement date, any significant Project milestones, and the anticipated Project Completion date.

4 Price and Payment

The total price for the Project is \$2,535,000 (the “Project Price”) for the deliverables and services described in this SOW. Client is exempt from sales taxes and shall provide NEC with a valid sales tax exemption certificate prior to the date of invoice.

NEC will invoice Client for the Project Price in accordance with the billing schedule below. Unless otherwise expressly agreed to by NEC in writing, payments are due within thirty (30) days from the date of invoice.

Table 6: Billing Schedule

Milestone	Payment Amount
Contract Execution (10%)	\$253,500
Signed Scope of Work (20%)	\$507,000
System Delivery (30%)	\$760,500
Completion of System Acceptance Testing (SAT) (20%)	\$507,000
Final System Acceptance (20%)	\$507,000
Total	\$2,535,000

The total price for the annual maintenance for the Project is \$520,000 (the “Annual Maintenance Price”) as described in this SOW. Client is exempt from sales taxes and shall provide NEC with a valid sales tax exemption certificate prior to the date of invoice.

NEC will invoice Client for the Annual Maintenance Price upon completion of the warranty period and annually thereafter. Unless otherwise expressly agreed to by NEC in writing, payments are due within thirty (30) days from the date of invoice.

NEC will invoice the Client the annual maintenance fee of \$548,607.33 for the legacy Integra-ID AFIS system. This fee will cover maintenance and support services for the period between January 5, 2024 and January 4, 2025. If the legacy Integra-ID AFIS system is still in operational use after January 4, 2025, NEC will invoice the Client \$548,607.33 to cover the maintenance and support services for the period between January 5, 2025 and January 4 2026.

5 Complete Contract

This SOW, along with the Agreement, is the complete agreement between the parties concerning the Project and supersedes any prior oral or written communications between the parties with regard to the subject matter contained herein. The provisions of this SOW govern only the subject matter hereof and shall not apply to any other subject matter covered by the Agreement.

6 Project Completion Checklist

A draft version of NEC's Project Completion Checklist has been attached as Schedule A.

Schedule A – Project Completion Checklist

When NEC has achieved Project Completion, NEC will submit this checklist to Client. If Client fails to provide a Punchlist or sign and return this checklist to NEC within ten (10) days of receipt, the Project will be complete and NEC will be entitled to invoice Client in accordance with the payment schedule in Section 4 of the SOW.

Implementation Tasks/Deliverables

Date

- | | |
|--|-------|
| 1. Contract Execution | _____ |
| 2. Signed Scope of Work | _____ |
| 3. System Delivery | _____ |
| 4. Completion of System Acceptance Testing | _____ |
| 5. Final System Acceptance | _____ |

This is to confirm that as of __/__/20__, NEC has completed Services and provided the Deliverables under the MBIS Upgrade – On Premise SOW effective __/__/20__.

Submitted By:

NEC Corporation of America

Metropolitan Nashville Police Department

By: _____

Name: _____

Title: _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

Schedule B – Pricing Catalog

Metro Nashville Government can purchase the following items during the contract term. Please note that this pricing is based on 2023 costs and is subject to change based on current market prices.

Item	Discount off Catalog Price
<p>IBW Tenprint Workstation - IBW Tenprint license, one-year warranty, shipping and installation.</p> <p>Does not include PC, monitor or flatbed scanner, which will provided by MNPDP</p>	3%
<p>IBW Latent Workstation - IBW Latent license, one-year warranty, shipping and installation.</p> <p>Does not include PC, monitor or flatbed scanner, which will provided by MNPDP</p>	3%
<p>FastID Workstation - FastID license, one-year warranty, shipping and installation.</p> <p>Does not include PC, monitor or flatbed scanner, which will provided by MNPDP</p>	3%
<p>SmartScan Ruggedized Kiosk - desktop PC, ruggedized/ motorized cabinet, single monitor, 500 ppi scanner, SmartScan license, one-year warranty, shipping and installation.</p>	3%
<p>SmartScan Desktop - desktop PC, single monitor, 500 ppi scanner, SmartScan license, one-year warranty, shipping and installation.</p>	3%
<p>Print Server - FBI-certified hardcard printer, one-year warranty, shipping and installation.</p> <p>Does not include PC, monitor or flatbed scanner, which will provided by MNPDP</p>	3%
<p>High Volume Scanning Workstation – High volume scanner, one-year warranty, shipping and installation.</p> <p>Does not include PC, monitor or flatbed scanner, which will provided by MNPDP</p>	3%
<p>Professional Services – Developer</p>	3%
<p>Professional Services – Project Manager</p>	3%
<p>Professional Services – Engineer</p>	3%
<p>Professional Services – Trainer</p>	3%

Schedule C – Workstation and Peripherals Specifications

Workstation	Specification
IBW Tenprint Workstation	<ul style="list-style-type: none"> • Dell Optiplex (or equivalent) • Intel iCore 7 • 16 GB Memory • 500 TB Hard Drive (SAS preferred) • Network Card • Monitor (two 24-inch recommended) • Windows 10 or Windows 11 Pro (preferred) • 5-year Dell Warranty • Epson V850 Flatbed Scanner
IBW Latent Workstation	<ul style="list-style-type: none"> • Dell Optiplex (or equivalent) • Intel iCore 7 • 16 GB Memory • 500 GB Hard Drive (SAS preferred) • Network Card • Monitor (two 24-inch recommended) • Windows 10 or Windows 11 Pro (preferred) • 5-year Dell Warranty • Epson V850 Flatbed Scanner
FastID Workstation	<ul style="list-style-type: none"> • Dell OptiPlex (or equivalent) • Intel iCore 5 • 8 GB Memory • Network Card • Monitor (20-inch recommended) • 320 GB SATA, 7200RPM • Windows 10 or Windows 11 Pro (preferred) • 5-year Dell Warranty • Integrated Biometrics Watson Mini (fingerprint scanner)
Print Server Workstation	<ul style="list-style-type: none"> • Dell OptiPlex (or equivalent) • Intel iCore 5 • 8 GB Memory • Network Card • Monitor (20-inch recommended) • 320 GB SATA, 7200RPM

	<ul style="list-style-type: none"> • Windows 10 or Windows 11 Pro (preferred) • 5-year Dell Warranty
High Volume Scanner Workstation	<ul style="list-style-type: none"> • Dell OptiPlex (or equivalent) • Intel iCore 5 • 8 GB Memory • Network Card • Monitor (20-inch recommended) • 320 GB SATA, 7200RPM • Windows 10 or Windows 11 Pro (preferred) • 5-year Dell Warranty
Network Printer / Card Printer	<ul style="list-style-type: none"> • Lexmark MS821dn

Due to ongoing supply chain issues, NEC may need to substitute items of equipment and software (“Substitutions”), provided that such substitution will not adversely affect the functionality and performance of the deliverables. Substitutions do not adjust a fixed priced contract. NEC will provide written notification of such changes.

Schedule D – NEC Biometrics Software Release Policy

NEC's software release policy follows an industry standard process. The main activities involved in Release Management are:

- Developing new versions.
- Establishing a planning policy for the implementation of new versions.
- Testing new versions in an environment that simulates the live environment as closely as possible.
- Validating the new versions.
- Implementing new versions in the live environment.
- Version control.

The software release version is identified by three numbers. For example, software release 4.6.1:

- “4” reflects a version of a major release of software
- “6” reflects a version of a minor release of software
- “1” reflects a version of a supplemental release of software

NEC's policy for system upgrades are provided on an if-and-when available basis as follows:

Supplemental Releases - are defined as releases that materially affect the operational performance or functional performance of the software, for example, via patches and issue fixes (e.g., from version 5.0 to 5.0.1). All NEC clients are entitled to all such releases without any expense. All expenses for software, and professional services required for installation of such supplemental releases, assuming clients has a Maintenance and Support Agreement with NEC, will be covered by NEC.

Minor Releases or Enhancements - are defined as releases that improve or augment the utility, efficiency, performance, or functional capability of the software (e.g., from version 5.0 to 5.1). NEC clients are entitled to receive this software release free of charge, again assuming a subcontract agreement, which includes maintenance and support, is in effect. All expenses for software, and professional services required for installation of such Releases, assuming client has a subcontract agreement, which includes maintenance and support with NEC, will be covered by NEC.

Major Releases - are defined as releases that, in whole or in part, introduce new advances in technology (e.g., the introduction of a newer matching algorithm). Major releases reflect significant improvements in the software product, for which the client is responsible for all software, and professional services, including all applicable license fees required for implementation of the release. In NEC's discretion, license fees for upgrading to a Major Release may be discounted for clients with a current subcontract agreement, which includes maintenance and support and/or such releases may be made available for a limited period of time only. NEC will charge no more than \$200 per hour for professional services needed to implement major releases.

The following are not covered by software support:

- Any problem resulting from the misuse, improper use, alteration, or damage of the software;
- Any problem caused by modifications in any version of the software not made or authorized by NEC;
- Any problem resulting from programming other than the software supplied by NEC; or
- Any problem resulting from the combination of the software with other programming or systems as referenced by above to the extent such combination has not been approved by NEC.
- Client shall be responsible to pay NEC's normal charges and expenses for time or other resources provided by NEC to diagnose or attempt to correct any such problem.

EXHIBIT C**BIOMETRIC MASTER PURCHASE AND SALES AGREEMENT**

This Biometric Master Purchase and Sales Agreement (“Agreement”) is made part of the Master Contract between **NEC Corporation of America** (“NEC”) and **Metropolitan Government of Nashville and Davidson County** (“Customer”) (collectively, the “Parties” or individually a “Party”) and is as follows:

1. DEFINITIONS:

- 1.1** “**Appendix**” means any document attached and incorporated into this Agreement or attached and incorporated into any Order, outlining supplemental terms and conditions specific to certain Equipment, Software, and/or Service(s) (e.g. software license agreements, specific Equipment and/or Service warranties, etc.) or to other aspects of an applicable Order, and duly executed by the Parties.
- 1.2** “**Equipment**” means hardware products sold to Customer by NEC hereunder.
- 1.3** “**Final Acceptance**” shall mean Customer’s written acceptance of any deliverables, and Services or other work, including System acceptance testing, if applicable, provided by NEC to Customer.
- 1.4** “**NEC Affiliate**” means a corporation or other entity controlling, controlled by, or under common control with NEC either now or in the future. For the purposes of this definition, “control” means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity whether through the ownership of voting securities of such entity, by contract, or otherwise.
- 1.5** “**Order(s)**” shall collectively and individually refer to a variety of documents addressing business terms related to NEC’s provisioning of Software, Equipment, and/or Services, including but not limited to service descriptions, Statement(s) of Work, Purchase Order(s), or other similar order forms, each of which, when duly accepted and executed by authorized representatives of both Parties, shall be deemed incorporated herein. In the event of a conflict between the Order(s) and the terms of this Agreement, the terms of this Agreement shall prevail unless otherwise expressly agreed to by the Parties in writing.
- 1.6** “**Productive Use**” means the actual use of the Solution in the Customer’s operational environment for the performance of Customer’s operations.
- 1.7** “**Purchase Order**” means a Customer-issued document used for ordering Software, Equipment, and/or Services under this Agreement. All Purchase Orders are subject to review and acceptance by an authorized representative of NEC. No preprinted Purchase Order terms shall be binding upon NEC, unless otherwise expressly agreed to in writing by an authorized representative of NEC.
- 1.8** “**Services**” means any services provided by NEC under this Agreement, including maintenance, professional, or other related services performed for Customer by NEC hereunder.
- 1.9** “**Software**” means the machine-readable object code software programs licensed to Customer by NEC or its suppliers.
- 1.10** “**Solution**” means the System and Services contemplated by this Agreement as set forth in the Statement of Work.
- 1.11** “**System**” means the architectural and operational environment for the Solution provided by NEC or Customer meeting the requirements of this Agreement and the Statement of Work and related documentation, including Software and System Equipment.

- 1.12 **“Statement of Work”** or **“SOW”** means a tasking document that specifies the Services to be performed by NEC for Customer with respect to a specific project or engagement. More specifically, a Statement of Work is intended to clearly define the basic requirements and objectives of a project, and set the scope and boundaries of such project, including but not limited to, what work will be done, when it will be performed, and the roles and responsibilities of the Parties.
- 1.13 **“Third Party Software”** means any software of third parties provided by NEC to Customer under this Agreement as part of the Solution.
2. **GENERAL.** The provisions of this document (hereinafter “Base Agreement”), including all Appendices and Orders, collectively form and hereinafter are referred to as the “Agreement” and establish the general terms and conditions under which NEC shall sell and/or license Software, Equipment, and/or perform Services for, Customer. In the event of any conflict, ambiguity, or inconsistency in the definition or interpretation of any word, responsibility, obligation, deliverable, Service, or otherwise, between this Base Agreement and any Appendix or Order, such conflict or inconsistency shall be resolved by giving precedence in the following order: (1) this Base Agreement; (2) the applicable Appendix; or (3) Order, including Statements of Work.

This Agreement includes the following Appendix:

- **Appendix A Pricing and Payment Schedule**
3. **TERM.** The term of this Agreement shall commence on the Effective Date and shall continue for a period of **three (3)** years (“Initial Term”) unless otherwise terminated as outlined herein. This Agreement may be extended by a letter or amendment signed by both parties. The option to extend may be exercised by, and at the discretion, of the Customer. However, in no event shall the term of the extension exceed sixty (60) months.
4. **SOFTWARE LICENSE GRANT.** Subject to the other applicable provisions in this Agreement, including but not limited to the payment of licensing fees, licensing term, and capacity and usage, NEC grants Customer a non-exclusive, limited, non-transferable license to install and use (in object code form only) the NEC Software for Customer’s internal business purposes. The Parties may agree to any other terms as set forth in a Software-specific Appendix to the applicable Order.
5. **LICENSE RESTRICTIONS.** Customer may not do the following: (i) modify, adapt, translate, or create derivative works based upon the Software; (ii) reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of the Software except to the extent you may be expressly permitted to reverse engineer or decompile under applicable law; (iii) sell, rent, lease, timeshare, provide subscription services, lend, sublicense, distribute, assign, or otherwise transfer any rights in the Software; and (iv) disclose or publish results of any benchmark tests of any Software to any third party without NEC’s prior written consent. Except as otherwise expressly permitted under this Agreement, Customer shall not have any rights to use any NEC Software, in whole or in part, for any other use or purpose whatsoever and any right not expressly provided to Customer under this Agreement shall be reserved by NEC. The Software will be used for identification and/or facial recognition purposes only and will not be used and implemented in direct connection with armed weapons.

To ensure compliance with this Agreement, upon forty-five (45) days written notice, NEC shall have the right to audit Customer’s use of the Software.

6. **PAYMENT.** Unless otherwise expressly agreed to by the Parties in writing, all payments are due within sixty (60) days from the date of an invoice and in accordance with the Pricing and Payment Schedule attached hereto as Appendix A. All invoices will be sent to Customer via email (“E-Invoicing”) using the email address(es) of the contact(s) provided to NEC by Customer, unless Customer expressly elects to opt out of E-Invoicing. If Customer changes its contact(s) for the receipt of E-Invoicing, Customer will promptly notify NEC of such change.

If Customer fails to pay the undisputed portion of any invoice within the time specified, to the extent permitted by Tennessee law, NEC may charge Customer interest equal to the lesser of 1.5% per month [eighteen percent (18%) per annum] or the maximum rate allowed by law on such undisputed portion. NEC's provision of Software, Equipment, and/or Services is subject to credit approval for each transaction. Customer understands that any information obtained by NEC from any third party credit bureau for the purpose of verifying Customer's creditworthiness will be held in confidence and will remain the property of NEC, whether or not credit is extended.

- 7. LIMITATION OF LIABILITY.** TO THE EXTENT PERMITTED BY TENNESSEE LAW, EXCEPT FOR EITHER PARTY'S LIABILITIES ARISING FROM USE OF INTELLECTUAL PROPERTY BEYOND THE SCOPE PERMITTED BY THIS AGREEMENT, AND SUBJECT TO APPLICABLE TENNESSEE LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR DAMAGES EXCEEDING THE FEES PAID OR OWED TO THE OTHER PARTY UNDER THE TRANSACTION GIVING RISE TO THE CLAIM; AND TO EXTENT PERMITTED BY TENNESSEE LAW, NEITHER PARTY SHALL HAVE ANY LIABILITY FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, PUNITIVE, OR SPECIAL DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE), ARISING OUT OF THIS AGREEMENT, (INCLUDING ANY DAMAGES ARISING UNDER ANY CLAIM OR NEGLIGENCE, STRICT LIABILITY, OR OTHER THEORY), EVEN IF THE PARTY INCURRING SUCH DAMAGES HAS ADVISED THE OTHER PARTY OF THE POSSIBILITY OF SUCH DAMAGES..

8. LIMITED WARRANTY.

EQUIPMENT. NEC represents and warrants that all Equipment manufactured by NEC, or an NEC Affiliate, will be free from defects in material and workmanship and will operate substantially in accordance with manufacturers' specifications for the period stated in the applicable Order. For Equipment not manufactured by NEC or an NEC Affiliate, NEC will pass the manufacturer's warranty through to Customer to the extent NEC is lawfully permitted to do so. Additional warranty terms may be included in an Equipment-specific Appendix to the applicable Order.

SERVICES. NEC represents and warrants that all Services provided to Customer pursuant to any Order shall be performed by competent personnel, with professional diligence and skill, consistent with industry standards, and will conform in all material respects to the specifications and requirements set forth, and for the period stated or incorporated, in the applicable Order. Additional warranty terms may be included in a Service-specific Appendix to the applicable Order.

SOFTWARE. NEC DOES NOT WARRANT THAT ANY NEC SOFTWARE PRODUCT PROVIDED WILL MEET CUSTOMER'S REQUIREMENTS OR THAT OPERATION OF ANY SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. EACH NEC SOFTWARE PRODUCT IS PROVIDED BY NEC "AS IS". THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF EACH NEC SOFTWARE PRODUCT SHALL BE WITH CUSTOMER.

TO THE EXTENT PERMITTED BY TENNESSEE LAW, EXCEPT AS SPECIFICALLY PROVIDED IN THIS AGREEMENT AND THE APPLICABLE APPENDIX AND/OR ORDER, NEC DISCLAIMS AND EXCLUDES TO THE FULL EXTENT PERMISSIBLE ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY WITH RESPECT TO THE SOFTWARE, EQUIPMENT, AND/OR SERVICES COVERED HEREUNDER. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY NEC SHALL CREATE A WARRANTY AND CUSTOMER MAY NOT RELY UPON SUCH INFORMATION OR ADVICE, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF SATISFACTORY QUALITY, AND NON INFRINGEMENT. NEC PARTICULARLY DISCLAIMS ALL WARRANTIES ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE, AND ALL WARRANTIES RELATED TO THIRD PARTY EQUIPMENT, MATERIAL, SERVICES, OR SOFTWARE NOT PROVIDED HEREUNDER ARE EXPRESSLY EXCLUDED. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THE AGREEMENT.

NO OTHER REPRESENTATIONS OR WARRANTIES; NON-RELIANCE EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES CONTAINED IN THIS SECTION OF THIS AGREEMENT, (A) NEC, NOR ANY OTHER PERSON ON NEC'S BEHALF, HAS MADE OR MAKES ANY EXPRESS OR IMPLIED REPRESENTATION OR WARRANTY REGARDING THE NEC PRODUCTS, EITHER ORAL OR WRITTEN, WHETHER ARISING BY LAW, COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE, TRADE OR OTHERWISE, ALL OF WHICH ARE EXPRESSLY DISCLAIMED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF TITLE AND NON-INFRINGEMENT, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND FITNESS OF THE NEC PRODUCTS FOR USE IN COMPLIANCE WITH APPLICABLE LAWS, REGULATIONS OR GOVERNMENTAL ORDERS GOVERNING OR RELATING TO SUCH USE, AND (B) CUSTOMER ACKNOWLEDGES THAT IT HAS NOT RELIED UPON ANY REPRESENTATION OR WARRANTY MADE BY NEC, OR ANY OTHER PERSON ON NEC'S BEHALF, EXCEPT AS SPECIFICALLY PROVIDED IN THIS SECTION OF THIS AGREEMENT. AS USED HEREIN, "NEC PRODUCTS" MEANS ANY NEC EQUIPMENT, SOFTWARE AND/OR SERVICES PROVIDED BY NEC UNDER THIS AGREEMENT, INCLUDING MAINTENANCE, PROFESSIONAL, OR OTHER RELATED SERVICES.

- 9. INTELLECTUAL PROPERTY INDEMNIFICATION (NEC).** Except as excluded below, NEC will defend and indemnify Customer against any third party claims or suits ("Actions") against Customer which allege infringement of a United States patent or copyright due to Customer's use of the Software, Equipment, and/or Services, provided that: (a) NEC is notified promptly in writing of the Action, (b) Metro may participate in the defense and settlement of any suit, (c) Customer fully cooperates in the defense when and as requested by NEC. Should Customer's continued use of Software, Equipment, and/or Services be enjoined, NEC may at its option and expense, either: (a) if commercially reasonable, procure for Customer the right to continue using the affected Software, Equipment, and/or Service(s), (b) replace or modify the same so that infringement is eliminated, or (c) If none of these alternatives are commercially reasonable, either party may terminate this Agreement and NEC shall issue a pro-rata refund of the licensing fee.

This indemnity shall not apply to any claims or suits concerning: (a) items manufactured by NEC at Customer's request and according to Customer's specifications, (b) use of Software, Equipment, and/or Services in a manner or for a purpose not contemplated by this Agreement, (c) equipment or software used by Customer in conjunction with the Equipment, but which was not supplied by NEC, or (d) commercial merchandise available on the open market or its equivalent. The foregoing provisions state the entire liability and obligations of each party, and the exclusive remedy of the other, with respect to any alleged intellectual property infringement hereunder.

In no event shall NEC be liable for any claims or demands attributable to the negligence or misconduct of Customer or failure of Customer to fulfill their responsibilities under this Agreement.

- 10. TERMINATION FOR CAUSE.** Either party may terminate this Agreement upon thirty (30) days' written notice if the other party materially breaches any term or condition of this Agreement or an Appendix and fails to cure the breach within thirty (30) days (fifteen (15) days in the event of payment default) following written notice specifying the breach. A material breach shall be deemed to occur (i) if Customer fails to pay any sum when due ("Termination for Non-payment"); or (ii) if either Party fails to perform or observe any material obligation or provision to be performed or observed herein ("Termination for Breach"). For purposes of this Agreement, a material obligation or provision shall be defined as one stated in this Agreement, the breach of which would likely cause the non-breaching party to suffer material harm to its business or reputation. Upon termination, Customer shall immediately remove and destroy all copies of the Software or any parts thereof.

- 11. MONETARY OBLIGATIONS UPON EARLY TERMINATION.** In the case of Termination for Non-payment or Termination for Breach resulting from the Customer's breach, any unpaid and accrued payment obligations of Customer shall survive and continue beyond Termination and NEC shall be considered to have earned all fees set forth in Appendix A and will be entitled to retain any fees that have already been paid by Customer.

- 12. THIRD PARTY BENEFICIARIES.** Customer acknowledges and agrees that NEC's Licensors are direct and intended third party beneficiaries of this Agreement.

- 13. ARCHIVAL/BACK-UP COPIES.** Customer may make one (1) copy of the NEC Software as necessary for backup and archival purposes only. All copies shall include any copyright and/or any other proprietary notices contained on the original NEC Software. Customer may not transfer the rights to a backup copy.
- 14. TECHNICAL SUPPORT.** NEC may provide Customer with technical support services, in accordance with the Maintenance Agreement, if selected by Customer.
- 15. PRODUCTIVE USE.** When applicable, the System shall achieve Go-Live and shall be ready for Productive Use when Customer approves, in writing, the deliverables within the Statement of Work. In the event any System, Equipment, or Software delivered after the date of execution of this Agreement is put into Productive Use by the Customer, notwithstanding any failure to pass any System acceptance test, and such Productive Use extends for a cumulative duration in excess of sixty (60) days, the applicable warranty provided shall commence and Customer shall pay the remaining balance of all monies due, the Solution shall then be deemed accepted.
- 16. SUBSTITUTION.** NEC may at any time before Final Acceptance, add, delete, and/or substitute items of Equipment and Software comprising the Solution (“Substitutions”), provided that such Substitutions will not adversely affect the functionality and performance of the Solution specified in NEC’s Proposal. Substitutions do not adjust a fixed priced contract.
- 17. STATEMENT OF WORK (“SOW”) CHANGES.** Customer may request changes in the SOW in connection with the performance of the Agreement. NEC will use commercially reasonable efforts to evaluate the implications of such changes, including, without limitation, the cost and schedule of any proposed changes.
- (i) If changes in design, workmanship, or material are of such a nature as to increase the cost of any part of the work, the price fixed in this Agreement will be adjusted by such amount as NEC and Customer agree upon as the reasonable and proper allowance for the adjustment in the cost of the work.
 - (ii) A change in the SOW will not be valid unless NEC has provided written approval of such change and the resulting adjustment in price has been agreed upon in writing by NEC and Customer. No oral statement of any person whatsoever shall in any manner or degree modify or otherwise affect the terms of this Agreement or the requirements of the SOW.

- 18. DELIVERY, TITLE, AND RISK OF LOSS.** The Equipment will be shipped via CPT Destination. NEC will select the carrier for shipment and Customer will bear the shipping costs as specified in Appendix A. Risk of loss shall pass to Customer upon shipment.

During the warranty period (as defined in Order-specific Appendix), NEC shall bear the cost of shipping and insurance when the Equipment is shipped for mechanical replacement or remedial maintenance purposes, unless such replacement was due to fault or negligence of NEC.

- 19. IMPORT EXPORT CONTROLS.** Customer hereby acknowledges that the Software and/or Equipment supplied hereunder may be subject to export controls under the laws and regulations of the United States (U.S.). Customer shall comply with such laws and regulations and agrees not to export, re-export, or transfer Software and/or Equipment without first obtaining all required U.S. Government authorizations or licenses. NEC and Customer each agree to provide the other such information and assistance as may reasonably be required by the other in connection with securing such authorizations or licenses, and to take timely action to obtain all required support documents.

Customer hereby certifies that the Software and/or Equipment sold or licensed hereunder are sold or licensed to Customer as a final purchaser or licensee that is acquiring such Software and/or Equipment for its own internal use and not for resale, remarketing, or distribution. Customer further certifies none of the Software or Equipment supplied to Customer hereunder will be exported, re-exported, or otherwise transferred by Customer:

- To a U.S. embargoed or highly restricted destination (15 United States Code of Federal Regulations ("CFR") Part 746)
- For use by or for any military end-user, or in any military end-use located in or operating under the authority of any country identified in Country Group D1 under 15 CFR, Supplement No. 1 to Part 740 (15 CFR Part 740)
- To, or made available by Customer for use by or for, any entity that is engaged in the design, development, production, stockpile, or use of nuclear, biological, or chemical weapons or missiles (15 CFR Part 744)
- To parties on any of the following U.S. Government's lists of denied persons, without first obtaining all required U.S. Government authorizations or licenses.

Denied Parties List:

<http://www.bis.doc.gov/dpl/thedeniallist.asp>

Unverified List:

http://www.bis.doc.gov/enforcement/unverifiedlist/unverified_parties.html

Entity List:

<http://www.access.gpo.gov/bis/ear/pdf/744spir.pdf>

Specially Designated Nationals List:

<http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf>

Debarred List:

<http://www.pmdtc.state.gov/compliance/debar.html>

Nonproliferation Sanctions: <http://www.state.gov/t/isn/c15231.htm#>

Customer's obligation under this clause shall survive the expiration or termination of this Agreement. Customer agrees to maintain a record of exports, re-exports, and transfers of the Equipment for five (5) years and to forward within that time period any required records to NEC or, at NEC's request, to the U.S. Government. Customer agrees to permit audits by NEC or the U.S. Government as required under the applicable regulations to ensure compliance with this Agreement.

- 20. FORCE MAJEURE.** Except for the obligation to pay monies due and owing, neither Party shall be responsible for any failure to perform or delay in performing any of its obligations hereunder where and

to the extent that such failure or delay results from causes outside the reasonable control of the Party, including but not limited to governmental actions, acts of terrorism, epidemics, pandemics, transportation or labor strikes, environmental conditions, fire, flood, riot, strike, life or health-threatening conditions.

21. ALTERNATIVE DISPUTE RESOLUTION. The Parties shall attempt in good faith to resolve potential disputes informally and promptly in accordance with the following: (a) Senior Level Negotiations. Upon written request by either Party, the Parties shall attempt to resolve the dispute by negotiations between their designated senior representatives. The Parties shall meet as often as they deem reasonably necessary to exchange information and attempt to resolve the dispute; and (b) Arbitration. If, after good faith negotiations, the Parties have not resolved the dispute, the parties agree to submit the dispute to binding arbitration under the Federal Arbitration Act, 9 U.S.C. § 1, et seq., to the exclusion of state law inconsistent therewith.

Binding arbitration shall be before a single arbitrator agreed upon by the parties and shall take place in mutually agreed venue. The arbitration shall be administered by JAMS pursuant to its Comprehensive Arbitration Rules and Procedures. Any award of the Arbitrator is final and binding and judgment on the award may be entered in any court having jurisdiction. The parties agree to equally share the costs associated with the arbitration.

22. GOVERNING LAW. This Agreement will have been made, executed, and delivered in the State of Tennessee and will be governed and construed for all purposes in accordance with the laws of the State of Tennessee without giving effect to conflict of laws provisions. The parties specifically disclaim the United Nations Convention on Contracts for the International Sale of Goods.

23. CONFIDENTIALITY. "Confidential Information" as used herein, and subject to applicable Tennessee law, means non-public information that is exchanged between the Parties, provided that such information is: (i) labeled or identified "Confidential" at the time it is provided by the disclosing Party, or (ii) disclosed under circumstances that would indicate to a reasonable person that the information should be treated as confidential by the Party receiving the information. If the disclosing Party fails to identify information as "Confidential Information" at the time of disclosure it may subsequently identify the information as "Confidential Information" by giving written notice to the other Party.

Notwithstanding the foregoing definition, the term Confidential Information does not include information which: (i) has been published by the disclosing Party or is otherwise in the public domain through no fault of the receiving Party; (ii) is properly within the legitimate possession of the receiving Party prior to its disclosure hereunder and without any obligation of confidence; (iii) is lawfully received by receiving Party from a third party who lawfully possesses the information and who is not restricted from disclosing the Confidential Information to the receiving Party; (iv) is independently developed by the receiving Party without use of the Confidential Information; or (v) is approved for disclosure by the disclosing Party, in writing, prior to its disclosure.

Each Party understands and agrees that in the performance of Services under this Agreement, or in contemplation thereof, that a Party may have access to Confidential Information of the other Party. The receiving Party agrees that all Confidential Information disclosed by the other Party shall be held in confidence and used only in performance of Services under this Agreement. The receiving Party shall exercise the same standard of care to protect such Confidential Information as is used to protect its own proprietary data, but in no event, less than a reasonable standard of care.

Confidential Information may be disclosed in response to a valid order of a court or other governmental body or as otherwise required by law; provided, however, that the receiving Party first gives notice to the disclosing Party and has, as appropriate: (i) fully cooperated in the disclosing Party's attempt to obtain a "protective order" from the appropriate court or other governmental body, or (ii) attempted to classify the media containing the Confidential Information to prevent access by the public, in accordance with the provisions of the federal Freedom of Information Act ("FOIA") or similar state statutes.

24. INTELLECTUAL PROPERTY OWNERSHIP, RESERVATION OF RIGHTS. Customer acknowledges and agrees that (i) Equipment and/or Services may contain, embody, or be based on, patented or patentable inventions, trade secrets, copyrights, and other intellectual property rights of NEC or the Equipment manufacturer, and that NEC or the manufacturer, respectively shall continue to be the sole owner of all Intellectual Property Rights in the Equipment. (ii) NEC and its licensors own and shall retain all rights, title, and interest in and to the NEC Software, including without limitation, all intellectual property rights embodied therein; and (iii) the NEC Software's structure, organization, sequence, and source code are the valuable trade secrets and confidential information of NEC and/or its licensors ("NEC Intellectual Property").

The NEC Software is protected by law, including without limitation the copyright laws of the United States and other countries, and by international treaty provisions. Except as expressly stated herein, this license does not grant Customer any intellectual property rights in the NEC Software and all rights not expressly granted are reserved by NEC and its licensors. Customer agrees not to remove or obliterate any copyright, trademark, or other proprietary rights notices contained in or on the NEC Software.

Unless otherwise expressly agreed in writing by the Parties in a separate Appendix, including a Statement of Work, should NEC, as a result of performing Services under an Order, create or discover new know-how, techniques, or other intellectual property ("New IP"), NEC shall own this New IP.

25. RELATIONSHIP OF THE PARTIES. NEC undertakes performing its obligations pursuant to this Agreement as an independent contractor. Nothing contained herein or done pursuant to this Agreement shall make either Party or its agents or employees the legal representative, agent, or employee of any other Party for any purpose whatsoever.

26. SECTION HEADINGS. The section headings contained herein are for convenience in reference and are not intended to define or limit the scope of any provision of this Agreement.

27. SEVERABILITY. If any provision of this Agreement is for any reason held to be unenforceable, all other provisions of this Agreement will remain in full force and effect and the unenforceable provision shall be replaced by a mutually acceptable enforceable provision consistent with the Parties' original intent.

28. SURVIVAL OF OBLIGATIONS. The respective obligations of Customer and NEC under this Agreement which by their nature would continue beyond the termination, cancellation, or expiration of the Agreement, shall survive termination, cancellation, or expiration.

29. FACSIMILE AND ELECTRONIC SIGNATURES. NEC and Customer hereby agree to regard facsimile representations of original signatures and electronic signatures of authorized officials of each party, as legally sufficient, and that the Parties need not follow up facsimile transmissions and electronic signatures of such documents by subsequent transmissions of "original" versions of such documents.

30. U.S. GOVERNMENT RIGHTS. The Software was developed entirely at private expense. The Software licensed under this Agreement is "commercial computer software" as the term is described in 48 C.F.R. 252.227-7014(a)(1). If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of this Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 48 C.F.R. 12.211 (Technical Data) of the Federal Acquisition Regulations ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of this License Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFAR") and its successors.

31. WAIVER OF TERMS AND CONDITIONS. Failure of either Party to enforce any of the terms or conditions of this Agreement shall not constitute a waiver of any such terms or conditions, or of any other terms or conditions.

32. COMPLIANCE WITH LAWS. Customer shall (a) comply with all applicable laws, regulations and governmental orders governing or relating to the use of the deliverables and services, including, but without limitation, all applicable privacy and data protection laws, and (b) at its own expense, obtain and maintain in full force and effect throughout the continuance of this Agreement, all licenses, permits, authorizations, approvals and government filings and registrations necessary or appropriate for the exercise of its rights and the performance of its obligations under this Agreement and for use of the deliverables and services.

Affidavits

Compliance with Laws: After first being duly sworn according to law, the undersigned (Affiant) states that he/she and the contracting organization is presently in compliance with, and will continue to maintain compliance with, all applicable federal, state, and local laws.

Taxes and Licensure: Affiant states that Contractor has all applicable licenses, including business licenses. Affiant also states that Contractor is current on its payment of all applicable gross receipt taxes and personal property taxes. M.C.L. 4.20.065

Nondiscrimination: Affiant affirms that by its employment policy, standards and practices, it does not subscribe to any personnel policy which permits or allows for the promotion, demotion, employment, dismissal or laying off of any individual due to race, creed, color, national origin, age or sex, and are not in violation of, and will not violate, any applicable laws concerning the employment of individuals with disabilities. M.C.L. 4.28.020

Employment Requirement: Affiant affirms that Contactor's employment practices are in compliance with applicable United States immigrations laws. M.C.L. 4.40.060.

Covenant of Nondiscrimination: Affiant affirms that in consideration of the privilege to submit offers in response to this solicitation, we hereby consent, covenant, and agree as follows:
To adopt the policies of the Metropolitan Government relating to equal opportunity in contracting on projects and contracts funded, in whole or in part, with funds of the Metropolitan Government;
- To attempt certain good faith efforts to solicit Minority-owned and Woman-owned business participation on projects and contracts in addition to regular and customary solicitation efforts;
- Not to otherwise engage in discriminatory conduct;
- To provide a discrimination-free working environment;
- That this Covenant of Nondiscrimination shall be continuing in nature and shall remain in full force and effect without interruption;
- That the Covenant of Nondiscrimination shall be incorporated by reference into any contract or portion thereof which the Supplier may hereafter obtain; and
- That the failure of the Supplier to satisfactorily discharge any of the promises of nondiscrimination as made and set forth herein shall constitute a material breach of contract. M.C.L. 4.46.070

Contingent Fees: It is a breach of ethical standards for a person to be retained, or to retain a person, to solicit or secure a Metro contract upon an agreement or understanding for a contingent commission, percentage, or brokerage fee, except for retention of bona fide employees or bona fide established commercial selling agencies for the purpose of securing business. After first being duly sworn according to law, the undersigned Affiant states that the Contractor has not retained anyone in violation of the foregoing. M.C.L. 4.48.080

Iran Divestment Act Affidavit: By submission of this offer and in response to the solicitation, Contractor(s) and each person signing on behalf of Contractor(s) affirm, under penalty of perjury, that to the best of their knowledge and belief, neither the Contractor(s), nor proposed subcontractors, subconsultants, partners and any joint venturers, are on the list created pursuant to the Tennessee Code Annotated § 12-12-106 (Iran Divestment Act). Referenced website:

https://www.tn.gov/content/dam/tn/generalservices/documents/cpo/library/2022/List_of_persons_pursuant_to_Tenn._Code_Ann._12-12-106_Iran_Divestment_Act_updated_with%20NY05.04.22.pdf

Sexual Harassment: Affiant affirms that should it be awarded a contract with the Metropolitan Government for a period of more than twelve (12) months and/or valued at over five hundred thousand (\$500,000) dollars, affiant shall be required to provide sexual harassment awareness and prevention training to its employees if those employees:

1. Have direct interactions with employees of the Metropolitan Government through email, phone, or in-person contact on a regular basis;
2. Have contact with the public such that the public may believe the contractor is an employee of the Metropolitan Government, including but not limited to a contractor with a phone number or email address associated with Metropolitan government or contractors with uniforms or vehicles bearing insignia of the Metropolitan Government; or
3. Work on property owned by the metropolitan government.

Such training shall be provided no later than (90) days of the effective date of the contract or (90) days of the employee's start date of employment with affiant if said employment occurs after the effective date of the contract. M.C.L. 2.230.020.

Affiant affirms that Contractor is not currently, and will not for the duration of the awarded Contract, engage in a boycott of Israel for any awarded contract that meets the following criteria:

- Has total potential value of two hundred fifty thousand (\$250,000) or more;
- Affiant has ten (10) or more employees.

Affiant affirms that offeror is and will remain in compliance with the provisions of Chapter 4.12 of the Metro Procurement Code and the contents of its offer as submitted. Affiant further affirms that offeror understands that failure to remain in such compliance shall constitute a material breach of its agreement with the Metropolitan Government.

And Further Affiant Sayeth Not:

Organization Name: NEC Corporation of America

Organization Officer Signature: Eugene Le Roux

Name of Organization Officer: Eugene Le Roux

Title: VP Government and International



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 06/14/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER MARSH USA LLC. 155 N. WACKER, SUITE 1200 CHICAGO, IL 60661 CN101822795-Std-Cyber-24-25	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2">CONTACT NAME: Marsh U.S. Operations</td> </tr> <tr> <td>PHONE (A/C No. Ext): 866-966-4664</td> <td>FAX (A/C, No): 212-948-0770</td> </tr> <tr> <td colspan="2">E-MAIL ADDRESS: Chicago.CertRequest@marsh.com</td> </tr> </table> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">INSURER(S) AFFORDING COVERAGE</th> <th style="text-align: center;">NAIC #</th> </tr> </thead> <tbody> <tr> <td>INSURER A : Mitsui Sumitomo Insurance Co. Of America</td> <td style="text-align: center;">20362</td> </tr> <tr> <td>INSURER B : Mitsui Sumitomo Insurance USA, Inc.</td> <td style="text-align: center;">22551</td> </tr> <tr> <td>INSURER C :</td> <td></td> </tr> <tr> <td>INSURER D :</td> <td></td> </tr> <tr> <td>INSURER E :</td> <td></td> </tr> <tr> <td>INSURER F :</td> <td></td> </tr> </tbody> </table>	CONTACT NAME: Marsh U.S. Operations		PHONE (A/C No. Ext): 866-966-4664	FAX (A/C, No): 212-948-0770	E-MAIL ADDRESS: Chicago.CertRequest@marsh.com		INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A : Mitsui Sumitomo Insurance Co. Of America	20362	INSURER B : Mitsui Sumitomo Insurance USA, Inc.	22551	INSURER C :		INSURER D :		INSURER E :		INSURER F :	
CONTACT NAME: Marsh U.S. Operations																					
PHONE (A/C No. Ext): 866-966-4664	FAX (A/C, No): 212-948-0770																				
E-MAIL ADDRESS: Chicago.CertRequest@marsh.com																					
INSURER(S) AFFORDING COVERAGE	NAIC #																				
INSURER A : Mitsui Sumitomo Insurance Co. Of America	20362																				
INSURER B : Mitsui Sumitomo Insurance USA, Inc.	22551																				
INSURER C :																					
INSURER D :																					
INSURER E :																					
INSURER F :																					

COVERAGES **CERTIFICATE NUMBER:** CHI-010381535-07 **REVISION NUMBER:** 4

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS														
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input checked="" type="checkbox"/> LOC OTHER:			PKG3101192	04/01/2024	04/01/2025	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>EACH OCCURRENCE</td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>DAMAGE TO RENTED PREMISES (Ea occurrence)</td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>MED EXP (Any one person)</td><td style="text-align: right;">\$ 10,000</td></tr> <tr><td>PERSONAL & ADV INJURY</td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>GENERAL AGGREGATE</td><td style="text-align: right;">\$ 2,000,000</td></tr> <tr><td>PRODUCTS - COMP/OP AGG</td><td style="text-align: right;">\$ 2,000,000</td></tr> <tr><td></td><td style="text-align: right;">\$</td></tr> </table>	EACH OCCURRENCE	\$ 1,000,000	DAMAGE TO RENTED PREMISES (Ea occurrence)	\$ 1,000,000	MED EXP (Any one person)	\$ 10,000	PERSONAL & ADV INJURY	\$ 1,000,000	GENERAL AGGREGATE	\$ 2,000,000	PRODUCTS - COMP/OP AGG	\$ 2,000,000		\$
EACH OCCURRENCE	\$ 1,000,000																				
DAMAGE TO RENTED PREMISES (Ea occurrence)	\$ 1,000,000																				
MED EXP (Any one person)	\$ 10,000																				
PERSONAL & ADV INJURY	\$ 1,000,000																				
GENERAL AGGREGATE	\$ 2,000,000																				
PRODUCTS - COMP/OP AGG	\$ 2,000,000																				
	\$																				
A	AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY			BVR8304045 BVM8803120	04/01/2024 04/01/2024	04/01/2025 04/01/2025	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>COMBINED SINGLE LIMIT (Ea accident)</td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>BODILY INJURY (Per person)</td><td style="text-align: right;">\$</td></tr> <tr><td>BODILY INJURY (Per accident)</td><td style="text-align: right;">\$</td></tr> <tr><td>PROPERTY DAMAGE (Per accident)</td><td style="text-align: right;">\$</td></tr> <tr><td>COMP/COLL DED.</td><td style="text-align: right;">\$ 1,000</td></tr> </table>	COMBINED SINGLE LIMIT (Ea accident)	\$ 1,000,000	BODILY INJURY (Per person)	\$	BODILY INJURY (Per accident)	\$	PROPERTY DAMAGE (Per accident)	\$	COMP/COLL DED.	\$ 1,000				
COMBINED SINGLE LIMIT (Ea accident)	\$ 1,000,000																				
BODILY INJURY (Per person)	\$																				
BODILY INJURY (Per accident)	\$																				
PROPERTY DAMAGE (Per accident)	\$																				
COMP/COLL DED.	\$ 1,000																				
B	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input type="checkbox"/> RETENTION \$			UMB5000517	04/01/2024	04/01/2025	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>EACH OCCURRENCE</td><td style="text-align: right;">\$ 5,000,000</td></tr> <tr><td>AGGREGATE</td><td style="text-align: right;">\$ 5,000,000</td></tr> <tr><td></td><td style="text-align: right;">\$</td></tr> </table>	EACH OCCURRENCE	\$ 5,000,000	AGGREGATE	\$ 5,000,000		\$								
EACH OCCURRENCE	\$ 5,000,000																				
AGGREGATE	\$ 5,000,000																				
	\$																				
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? <input checked="" type="checkbox"/> Y <input type="checkbox"/> N <input type="checkbox"/> N/A (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below			WCP9115732 WCP9115733 WCP9116950	04/01/2024 04/01/2024 04/01/2024	04/01/2025 04/01/2025 04/01/2025	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td><input checked="" type="checkbox"/> PER STATUTE</td> <td><input type="checkbox"/> OTHER</td> <td></td> </tr> <tr><td>E.L. EACH ACCIDENT</td><td></td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>E.L. DISEASE - EA EMPLOYEE</td><td></td><td style="text-align: right;">\$ 1,000,000</td></tr> <tr><td>E.L. DISEASE - POLICY LIMIT</td><td></td><td style="text-align: right;">\$ 1,000,000</td></tr> </table>	<input checked="" type="checkbox"/> PER STATUTE	<input type="checkbox"/> OTHER		E.L. EACH ACCIDENT		\$ 1,000,000	E.L. DISEASE - EA EMPLOYEE		\$ 1,000,000	E.L. DISEASE - POLICY LIMIT		\$ 1,000,000		
<input checked="" type="checkbox"/> PER STATUTE	<input type="checkbox"/> OTHER																				
E.L. EACH ACCIDENT		\$ 1,000,000																			
E.L. DISEASE - EA EMPLOYEE		\$ 1,000,000																			
E.L. DISEASE - POLICY LIMIT		\$ 1,000,000																			

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
 Re: Contract Number 6543886

Metropolitan Government of Nashville and Davidson County, its officials, officers, employees, and volunteers is/are included as additional insured where required by written contract with respect to General Liability and Auto Liability.

CERTIFICATE HOLDER Purchasing Agent Metropolitan Government of Nashville and Davidson County Metro Courthouse, Nashville, TN 37201	CANCELLATION SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE <div style="text-align: right;"><i>Marsh USA LLC</i></div>
---	--



ADDITIONAL REMARKS SCHEDULE

AGENCY MARSH USA LLC.		NAMED INSURED NEC Corporation of America 5205 N O' Conner Blvd Sutie 400 Irving, TX 75039	
POLICY NUMBER		EFFECTIVE DATE:	
CARRIER	NAIC CODE		

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
FORM NUMBER: 25 FORM TITLE: Certificate of Liability Insurance

CYBER TECH E&O
 Policy Number: MTP9031210.09
 Carrier: Indian Harbor Insurance Company
 Effective Date: 10/01/2023
 Expiration Date: 04/01/2025
 Technology Products and Services Limit: \$5,000,000; Retention \$250k
 Media Liability \$5,000,000 Limit; Retention \$250k
 Privacy & Cyber Security Limit: \$5,000,000; Retention \$250k
 Cyber-Extortion and Ransomware Limit: \$5,000,000; Retention \$250k
 Dependent BI \$2,500,000
 Dependent BI System Failure \$1,250,000

**METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY
DEPARTMENT OF FINANCE – PROCUREMENT
SOLE SOURCE JUSTIFICATION FORM**



SS #: SS2023152

Date Received: April 25, 2023

Send an email to PRG@nashville.gov and attach completed sole source form and supporting documentation.

Proposed supplier MUST be Registered in iProcurement

Date: 4/20/2023 Requesting Department/Agency/Commission: Police

Requesting Official: John Singleton Telephone #: 615-862-7702 This is for a multi-year contract.

Product/Service Description: Police Automated Fingerprint Identification System (AFIS) upgrade and support maintenance

Total Purchase (Enter the value for the entire contract life) Price: \$6,000,000

BU Number: 31401021 Fund #: 40021 Object Account: Any Other Accounting Info:

Proposed Supplier: NEC Corporation of America, a Nevada Corporation Proposed Supplier Contact: Kelly Gallagher

Supplier Address: 3929 W. John Carpenter Frwy City: Irving ST: TX Zip: 75063

Supplier Telephone #: 916-463-7003 Supplier Email: kelly.gallagher@necam.com

Metro Code: 4.12.060 Sole Source Procurement.

A contract may be awarded for a supply, service or construction item without competition when, under regulations promulgated by the standards board, the purchasing agent determines in writing that there is only one source for the required supply, service or construction item. The standards board may, by regulation, establish specific categories of supplies, services, or construction items as sole source items. (Ord. 92-210 § 1 (3-205), 1992)

R4.12.060.02 Conditions for Use of Sole Source Procurement.

Other, see explanation below

If Other, Explain Request: NEC is the sole developer and provider for the AFIS system currently in operation within MNPD since 1995. The system has custom interfaces developed to other critical Police department systems including RMS, Mugshot system, and the TBI AFIS system. This sole source procurement is required for compatability with the current database structure, equipment, custom interfaces, and manufacturer authorized support, warranty, and maintenance.

Signatures will be gotten by Procurement in DocuSign

Department Requester's Initials: JS

Requesting Department Director's Signature of Approval: John Drake

Date: 4/26/2023 | 7:50 AM CDT

SS2023152

SS #: _____

April 25, 2023

Date Received: _____

To be completed by the Procurement Division

Vetting & Research Needed; Date Requested by Purchasing Agent _____

Approval of Changes

PO **Multi-Year Contract**

ml

5/26/2023 | 5:10 PM CDT

Sole Source is Approved for: _____

Sole Source is Denied (See determination summary for denial reason)

5/12/2023 | 4:29 PM

PURCHASING AGENT: Michelle R. Hernandez Lane **Date:** _____



NEC Corporation of America
Biometrics Solutions Division
6535 N. State Hwy 161, 2nd Floor
Irving, TX 35039-2402

April 24, 2023

John Singleton
Police IT Director
Metro Nashville Police Department
Office: (615)862-7702

Mr. Singleton,

This letter is to confirm the sole source availability for the design, coding, configuration and implementation of the Metropolitan Nashville Police Department Integra-ID Automated Fingerprint Identification System located at the Metropolitan Nashville Police Department facility.

While input to the MNPd Integra AFIS and Archive solution supports open and National Standards functionality approved for use by the city, the database structures, software applications and algorithms are NEC proprietary. Furthermore, the design of the Integra AFIS and Archive databases can only be achieved through equipment and/or software provided by and maintained by NEC. No other vendor can modify proprietary data or make modification to products legally authorized to be marketed by NEC Corporation of America under penalty of patent infringement laws of the United States.

We do appreciate your confidence in NEC and our Biometrics products. Please do not hesitate to call me at 404-308-1166 if you have any further questions.

Sincerely,

A handwritten signature in black ink that reads 'Tom Markham'.

Tom Markham
Engineering Support Manager
Identification Solutions

Certificate Of Completion

Envelope Id: A1BDDDF01C09447CB3FA88F338F986BE	Status: Completed
Subject: Updated Sole Source Form - NEC Corp of America - SS2023152	
Source Envelope:	
Document Pages: 3	Signatures: 0
Certificate Pages: 15	Initials: 1
AutoNav: Enabled	Envelope Originator:
Envelopeld Stamping: Enabled	Procurement Resource Group
Time Zone: (UTC-06:00) Central Time (US & Canada)	730 2nd Ave. South 1st Floor
	Nashville, TN 37219
	prg@nashville.gov
	IP Address: 170.190.198.185

Record Tracking

Status: Original	Holder: Procurement Resource Group	Location: DocuSign
5/25/2023 5:03:46 PM	prg@nashville.gov	
Security Appliance Status: Connected	Pool: StateLocal	
Storage Appliance Status: Connected	Pool: Metropolitan Government of Nashville and Davidson County	Location: DocuSign

Signer Events

Signer Events	Signature	Timestamp
Michelle A Hernandez Lane michelle.lane@nashville.gov Chief Procurement Officer/Purchasing Agent Metro		Sent: 5/25/2023 5:05:22 PM Viewed: 5/26/2023 5:10:16 PM Signed: 5/26/2023 5:10:39 PM
Security Level: Email, Account Authentication (None)	Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events

In Person Signer Events	Signature	Timestamp

Editor Delivery Events

Editor Delivery Events	Status	Timestamp

Agent Delivery Events

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events

Certified Delivery Events	Status	Timestamp

Carbon Copy Events

Carbon Copy Events	Status	Timestamp
Judy Cantlon Judy.Cantlon@nashville.gov Security Level: Email, Account Authentication (None)		Sent: 5/26/2023 5:10:40 PM

Electronic Record and Signature Disclosure:
Accepted: 5/26/2023 8:59:01 AM
ID: 0755211f-2915-4ae3-9c72-d4b67ba488cc

Amber Gardner Amber.Gardner@nashville.gov Security Level: Email, Account Authentication (None)		Sent: 5/26/2023 5:10:40 PM
--	--	----------------------------

Electronic Record and Signature Disclosure:
Accepted: 12/26/2022 6:53:53 PM
ID: f39b7bb9-bb2b-47dd-b058-d2ecba0c41d3

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Terri L. Ray Terri.Ray@nashville.gov Finance Manager Metropolitan Government of Nashville and Davidson County Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign	COPIED	Sent: 5/26/2023 5:10:41 PM
--	---------------	----------------------------

John Singleton John.Singleton@nashville.gov Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Accepted: 5/18/2023 2:28:28 PM ID: 382ec53c-8257-4296-9471-64e4996f83e8	COPIED	Sent: 5/26/2023 5:10:41 PM Viewed: 5/26/2023 5:36:06 PM
---	---------------	--

Witness Events	Signature	Timestamp
----------------	-----------	-----------

Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
-------------------------	--------	------------

Envelope Sent	Hashed/Encrypted	5/25/2023 5:05:23 PM
Certified Delivered	Security Checked	5/26/2023 5:10:16 PM
Signing Complete	Security Checked	5/26/2023 5:10:39 PM
Completed	Security Checked	5/26/2023 5:10:42 PM

Payment Events	Status	Timestamps
----------------	--------	------------

Electronic Record and Signature Disclosure
--

Certificate Of Completion

Envelope Id: 1D45B0F4E42D46BDA2512AADE900EF1E	Status: Sent
Subject: Metro Contract 6543886 with NEC Corporation of America (Police)	
Source Envelope:	
Document Pages: 100	Signatures: 10
Certificate Pages: 18	Initials: 4
AutoNav: Enabled	Envelope Originator:
Enveloped Stamping: Enabled	Procurement Resource Group
Time Zone: (UTC-06:00) Central Time (US & Canada)	730 2nd Ave. South 1st Floor
	Nashville, TN 37219
	prg@nashville.gov
	IP Address: 170.190.198.185

Record Tracking


Status: Original 7/12/2024 9:03:30 AM	Holder: Procurement Resource Group prg@nashville.gov	Location: DocuSign
Security Appliance Status: Connected	Pool: StateLocal	
Storage Appliance Status: Connected	Pool: Metropolitan Government of Nashville and Davidson County	Location: DocuSign

Signer Events


Signer Events	Signature	Timestamp
Gary Clay Gary.Clay@nashville.gov Asst. Purchasing Agent Security Level: Email, Account Authentication (None)	 Signature Adoption: Uploaded Signature Image Using IP Address: 170.190.198.185	Sent: 7/22/2024 3:51:34 PM Viewed: 7/22/2024 4:32:19 PM Signed: 7/22/2024 4:32:58 PM

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

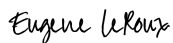
Samir Mehic samir.mehic@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 162.225.91.252 Signed using mobile	Sent: 7/22/2024 4:33:05 PM Viewed: 7/22/2024 5:17:44 PM Signed: 7/22/2024 5:18:23 PM
--	--	--

Electronic Record and Signature Disclosure:Accepted: 7/22/2024 5:17:44 PM
ID: 3b5b0995-9f33-43bb-b56c-77e095be2485

Ernest Franklin Ernest.Franklin@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 7/22/2024 5:18:26 PM Viewed: 7/23/2024 7:37:52 AM Signed: 7/23/2024 7:38:24 AM
--	--	--

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Eugene LeRoux eugene.leroux@necam.com Senior Vice President NEC Corporation of America Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 67.161.181.92 Signed using mobile	Sent: 7/23/2024 7:38:28 AM Viewed: 7/23/2024 8:19:46 AM Signed: 7/23/2024 8:27:42 AM
---	---	--

Electronic Record and Signature Disclosure:

Signer Events	Signature	Timestamp
---------------	-----------	-----------

Accepted: 7/23/2024 8:19:46 AM
ID: 17286ef2-d86a-4031-82a5-ab6f05b65fa0

Dennis Rowland
dennis.rowland@nashville.gov
Purchasing Agent & Chief Procurement Officer
Security Level: Email, Account Authentication (None)

Dennis Rowland

Signature Adoption: Pre-selected Style
Using IP Address: 170.190.198.185

Sent: 7/23/2024 8:27:46 AM
Viewed: 7/24/2024 6:49:17 AM
Signed: 7/24/2024 6:55:19 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Chief of Police John Drake
chiefofpolice@nashville.gov
Security Level: Email, Account Authentication (None)

Chief of Police John Drake

Signature Adoption: Pre-selected Style
Using IP Address: 170.190.198.104

Sent: 7/24/2024 6:55:23 AM
Viewed: 7/25/2024 10:51:28 AM
Signed: 7/25/2024 10:51:48 AM

Electronic Record and Signature Disclosure:
Accepted: 7/25/2024 10:51:28 AM
ID: e5a77b9b-7bc2-4092-8ac6-534d6929ecee

Kevin Crumbo/mal
michelle.Lane@nashville.gov
Deputy Director of Finance
Metro
Security Level: Email, Account Authentication (None)

Kevin Crumbo/mal

Signature Adoption: Pre-selected Style
Using IP Address: 170.190.198.185

Sent: 7/25/2024 10:51:53 AM
Viewed: 7/25/2024 1:21:53 PM
Signed: 7/29/2024 1:36:11 PM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Kevin Crumbo/mjw
MaryJo.Wiggins@nashville.gov
Security Level: Email, Account Authentication (None)

Kevin Crumbo/mjw

Signature Adoption: Pre-selected Style
Using IP Address: 170.190.198.100

Sent: 7/29/2024 1:36:20 PM
Viewed: 7/29/2024 1:45:24 PM
Signed: 7/29/2024 3:55:10 PM

Electronic Record and Signature Disclosure:
Accepted: 7/29/2024 3:46:40 PM
ID: b9648e69-444e-48a6-9150-806c8cf6523e

Balogun Cobb
balogun.cobb@nashville.gov
Security Level: Email, Account Authentication (None)

BC

Signature Adoption: Pre-selected Style
Using IP Address: 170.190.198.185

Sent: 7/29/2024 3:55:14 PM
Viewed: 7/29/2024 4:00:58 PM
Signed: 7/29/2024 4:01:06 PM

Electronic Record and Signature Disclosure:
Accepted: 7/29/2024 4:00:58 PM
ID: 34da3769-27c9-4276-8dea-91b5feae8e54

Tessa Ortiz-Marsh
tessa.ortiz-marsh@nashville.gov
Security Level: Email, Account Authentication (None)

Tessa Ortiz-Marsh

Signature Adoption: Pre-selected Style
Using IP Address: 170.190.198.144

Sent: 7/29/2024 4:01:14 PM
Viewed: 7/30/2024 9:04:39 AM
Signed: 7/30/2024 9:04:49 AM

Signer Events	Signature	Timestamp
---------------	-----------	-----------

Electronic Record and Signature Disclosure:
Accepted: 7/30/2024 9:04:39 AM
ID: f58cf8a3-4806-4552-bd1a-41e36eca6835

Tessa V. Ortiz-Marsh
tessa.ortiz-marsh@nashville.gov
Security Level: Email, Account Authentication
(None)



Sent: 7/30/2024 10:19:07 AM
Viewed: 7/30/2024 11:55:43 AM
Signed: 7/30/2024 11:55:51 AM

Signature Adoption: Pre-selected Style
Using IP Address: 170.190.198.144

Electronic Record and Signature Disclosure:
Accepted: 7/30/2024 11:55:43 AM
ID: e4195537-1864-4f39-ab9a-9deda05f3112

Procurement Resource Group
prg@nashville.gov
Metropolitan Government of Nashville and Davidson
County
Security Level: Email, Account Authentication
(None)

Sent: 7/30/2024 9:04:55 AM
Resent: 7/30/2024 11:55:55 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
-------------------------	-----------	-----------

Editor Delivery Events	Status	Timestamp
------------------------	--------	-----------

Agent Delivery Events	Status	Timestamp
-----------------------	--------	-----------

Intermediary Delivery Events	Status	Timestamp
------------------------------	--------	-----------

Certified Delivery Events	Status	Timestamp
---------------------------	--------	-----------

Carbon Copy Events	Status	Timestamp
--------------------	--------	-----------

Terri L. Ray
Terri.Ray@nashville.gov
Finance Manager
Metropolitan Government of Nashville and Davidson
County
Security Level: Email, Account Authentication
(None)

COPIED

Sent: 7/22/2024 3:51:34 PM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Kelly Gallagher
kelly.gallagher@necam.com
Security Level: Email, Account Authentication
(None)

COPIED

Sent: 7/23/2024 7:38:28 AM
Viewed: 7/23/2024 8:20:51 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Jemery Frye
jeremy.frye@nashville.gov
Security Level: Email, Account Authentication
(None)

Electronic Record and Signature Disclosure:
Accepted: 7/16/2024 9:19:29 AM
ID: 0cb5a982-7b02-470a-85a2-dc01f56e682b

Carbon Copy Events	Status	Timestamp
Kristin Heil Kristin.Heil@nashville.gov Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Amber Gardner Amber.Gardner@nashville.gov Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Austin Kyle publicrecords@nashville.gov Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Accepted: 7/25/2024 8:21:29 AM ID: 9aee4cb5-cb09-44ba-8788-10fd912c308c		
Terri Ray terri.ray@nashville.gov Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign		
Zak Kelley Zak.Kelley@Nashville.gov Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign		
John Singleton John.Singleton@nashville.gov Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Accepted: 7/3/2024 4:30:00 PM ID: a1f0e812-cb66-4ffc-a2bc-6ead2c73a714		
Shayla Johnson shayla.johnson@necam.com Security Level: Email, Account Authentication (None) Electronic Record and Signature Disclosure: Not Offered via DocuSign		

Witness Events	Signature	Timestamp
----------------	-----------	-----------

Notary Events	Signature	Timestamp
---------------	-----------	-----------

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	7/22/2024 3:51:34 PM
Envelope Updated	Security Checked	7/30/2024 10:19:06 AM
Envelope Updated	Security Checked	7/30/2024 10:19:06 AM

Payment Events	Status	Timestamps
----------------	--------	------------

