MIAMIBEACH

REQUEST FOR QUALIFICATIONS (RFQ)

RFQ NO. 2020-009-JC

Security Access Control System

RFQ ISSUANCE DATE: JANUARY 15, 2020

PROPOSALS DUE: FEBRUARY 20, 2020 AT 3:00 PM

ISSUED BY:

MIAMIBEACH

JASON CROUCH, PROCUREMENT CONTRACTING OFFICER
PROCUREMENT DEPARTMENT
1755 Meridian Avenue, 3rd Floor, Miami Beach, FL 33139
305.673.7000 x **26694** | jasoncrouch@miamibeachfl.gov | www.miamibeachfl.gov

MIAMIBEACH

TABLE OF CONTENTS

SECTION 0100 INSTRUCTIONS TO PROPOSERS

1. GENERAL. This Request for Qualifications (RFQ) is issued by the City of Miami Beach, Florida (the "City"), as the means for prospective Proposers to submit their qualifications, proposed scopes of work and cost proposals (the "proposal") to the City for the City's consideration as an option in achieving the required scope of services and requirements as noted herein. All documents released in connection with this solicitation, including all appendixes and addenda, whether included herein or released under separate cover, comprise the solicitation, and are complementary to one another and together establish the complete terms, conditions and obligations of the Proposers and, subsequently, the successful Proposer(s) (the "contractor[s]") if this RFQ results in an award.

The City utilizes **BidSync** (www.bidsync.com) (for automatic notification of competitive solicitation opportunities and document fulfillment, including the issuance of any addendum to this RFQ. Any prospective Bidder who has received this RFQ by any means other than through **BidSync** must register immediately with **BidSync** to assure it receives any addendum issued to this RFQ. Failure to receive an addendum may result in disqualification of proposal submitted. A BidSync document is attached for registration purposes, and in order to access all RFQ documents.

2. PURPOSE. Presently, the City operates a citywide physical access control security system (hereafter referred to as "access controls") that controls access to facilities. The current system is the based on Millennium Group software, which includes the primary function of granting door and facilities entry access by way of approved card credentials, thereby limiting physical access to buildings, offices, rooms, personnel, and City assets, as well as establish access rights. By way of this RFQ, the City intends to procure an access control system that is robust, and customizable in order to fully meet the needs of the City's security infrastructure. Additionally, the City will require routine and emergency services for the ongoing maintenance of the system.

Through this RFQ, the City intends to select a replacement citywide access control system (hardware, software, and maintenance) capable of providing the enhanced functionality for access control, system planning and integration, administration, credential management, hardware, training, support, and as further articulated in Appendix C. Interested parties are encouraged to submit qualifications and system details in accordance with Section 0300.

Following receipt and evaluation of proposals, the City Manager may recommend one or more bidders with whom the City may further consider during a negotiation phase to arrive at a mutually agreeable contract. The City may utilize the results of this RFQ to standardize access control operations.

3. ANTICIPATED RFQ TIMETABLE. The tentative schedule for this solicitation is as follows:

RFQ Issued	January 15, 2020
Pre-Proposal Meeting	January 29, 2020
Deadline for Receipt of Questions	February 10, 2020 by 5:00 PM
Responses Due	February 20, 2020 by 3:00 PM
Evaluation Committee Review	TBD

4. PROCUREMENT CONTACT. Any questions or clarifications concerning this solicitation shall be submitted to the Procurement Contact noted below:

Procurement Contact:	Telephone:	Email:
Jason Crouch	305-673-7000 x26694	jasoncrouch@miamibeachfl.gov

Additionally, the City Clerk is to be copied on all communications via e-mail at: RafaelGranado@miamibeachfl.gov; or via facsimile: 786-394-4188.

The Bid title/number shall be referenced on all correspondence. All questions or requests for clarification must be received no later than ten (10) calendar days prior to the date proposals are due as scheduled in Section 0200-3. All responses to questions/clarifications will be sent to all prospective Proposers in the form of an addendum.

5. PRE-PROPOSAL MEETING OR SITE VISIT(S). Only if deemed necessary by the City, a pre-proposal meeting or site visit(s) may be scheduled.

A Pre-PROPOSAL conference will be held as scheduled in Anticipated RFQ Timetable section above at the following address:

City of Miami Beach
Procurement Department
Conference Room
1755 Meridian Avenue, 3rd Floor
Miami Beach, Florida 33139

Attendance (in person or via telephone) is encouraged and recommended as a source of information, but is not mandatory. Proposers interested in participating in the Pre-Proposal Submission Meeting via telephone must follow these steps:

(1) Dial the TELEPHONE NUMBER: 1-877-873-8018 (Toll-free North America)
(2) Enter the MEETING NUMBER: 6312925

Proposers who are interested in participating via telephone should send an e-mail to the contact person listed in this RFQ expressing their intent to participate via telephone.

6. PRE-PROPOSAL INTERPRETATIONS. Oral information or responses to questions received by prospective Proposers are not binding on the City and will be without legal effect, including any information received at pre-submittal meeting or site visit(s). The City by means of Addenda will issue interpretations or written addenda clarifications considered necessary by the City in response to questions. Only questions answered by written addenda will be binding and may supersede terms noted in this solicitation. Addendum will be released through *BidSync.* Any prospective proposer who has received this RFQ by any means other than through *BidSync* must register immediately with *BidSync* to assure it receives any addendum issued to this RFQ. Failure to receive an addendum may result in disqualification of proposal. Written questions should be received no later than the date outlined in the **Anticipated RFQ Timetable** section.

7. CONE OF SILENCE. This RFQ is subject to, and all proposers are expected to be or become familiar with, the City's Cone of Silence Requirements, as codified in Section 2-486 of the City Code. Proposers shall be solely responsible for ensuring that all applicable provisions of the City's Cone of Silence are complied with, and shall be subject to any and all sanctions, as prescribed therein, including rendering their response voidable, in the event of such non-compliance. Communications regarding this solicitation are to be submitted in writing to the Procurement Contact named herein with a copy to the City Clerk at rafaelgranado@miamibeachfl.gov

8. ADDITIONAL INFORMATION OR CLARIFICATION. After proposal submittal, the City reserves the right to require additional information from Proposers (or Proposer team members or sub-consultants) to determine: qualifications (including, but not limited to, litigation history, regulatory action, or additional references); and financial capability (including, but not limited to, annual reviewed/audited financial statements with the auditors notes for each of their last two complete fiscal years).

9. PROPOSER'S RESPONSIBILITY. Before submitting a response, each Proposer shall be solely responsible for making any and all investigations, evaluations, and examinations, as it deems necessary, to ascertain all conditions and requirements affecting the full performance of the contract. Ignorance of such conditions and requirements, and/or failure to make such evaluations, investigations, and examinations, will not relieve the Proposer from any obligation to comply with every detail and with all provisions and requirements of the contract, and will not be accepted as a basis for any subsequent claim whatsoever for any monetary consideration on the part of the Proposer.

10. VETERAN BUSINESS ENTERPRISES PREFERENCE. Pursuant to City Code Section 2-374, the City shall give a preference to a responsive and responsible Proposer which is a small business concern owned and controlled by a veteran(s) or which is a service-disabled veteran business enterprise, and which is within five percent (5%) of the lowest responsive, responsible proposer, by providing such proposer an opportunity of providing said goods or contractual services for the lowest responsive proposal amount (or in this RFQ, the highest proposal amount).

11. DETERMINATION OF AWARD. The final ranking results of Phase II evaluation process will be considered by the City Manager who may recommend to the City Commission the Proposer(s) s/he deems to be in the best interest of the City or may recommend rejection of all proposals. The City Manager's recommendation need not be consistent with the scoring results identified herein and takes into consideration Miami Beach City Code Section 2-369, including the following considerations:

(1) The ability, capacity and skill of the Proposer to perform the contract.

(2) Whether the Proposer can perform the contract within the time specified, without delay or interference.

(3) The character, integrity, reputation, judgment, experience and efficiency of the Proposer.

(4) The quality of performance of previous contracts.

(5) The previous and existing compliance by the Proposer with laws and ordinances relating to the contract.

The City Commission shall consider the City Manager's recommendation and may approve such recommendation. The City Commission may also, at its option, reject the City Manager's recommendation and select another Proposal or Proposals which it deems to be in the best interest of the City, or it may also reject all Proposals.

12. NEGOTIATIONS. Following selection, the City reserves the right to enter into further negotiations with the selected Proposer. Notwithstanding the preceding, the City is in no way obligated to enter into a contract with the selected Proposer in the event the parties are unable to negotiate a contract. It is also understood and acknowledged by Proposers that no property, contract or legal rights of any kind shall be created at any time until and unless an Agreement has been agreed to; approved by the City; and executed by the parties.

SECTION 0200 GENERAL CONDITIONS

1. GENERAL DISCLAIMERS.

a. The solicitation referenced herein is being furnished to the recipient by the City of Miami Beach (the "City") for the recipient's convenience. Any action taken by the City in response to Proposals made pursuant to this solicitation, or in making any award, or in failing or refusing to make any award pursuant to such Proposals, or in cancelling awards, or in withdrawing or cancelling this solicitation, either before or after issuance of an award, shall be without any liability or obligation on the part of the City. In its sole discretion, the City may withdraw the solicitation either before or after receiving proposals, may accept or reject proposals, and may accept proposals which deviate from the solicitation, as it deems appropriate and in its best interest. In its sole discretion, the City may determine the qualifications and acceptability of any party or parties submitting Proposals in response to this solicitation.

b. The information contained herein is provided solely for the convenience of prospective Proposers. It is the responsibility of the recipient to assure itself that information contained herein is accurate and complete. The City does not provide any assurances as to the accuracy of any information in this solicitation. Any reliance on these contents, or on any permitted communications with City officials, shall be at the recipient's own risk. Proposers should rely exclusively on their own investigations, interpretations, and analyses. The solicitation is being provided by the City without any warranty or representation, express or implied, as to its content, its accuracy, or its completeness. No warranty or representation is made by the City or its agents that any Proposal conforming to these requirements will be selected for consideration, negotiation, or approval.

c. Bidders are hereby advised that this solicitation is subject to the following ordinances/resolutions, which may be found on the City Of Miami Beach website: http://web.miamibeachfl.gov/procurement/scroll.aspx?id=79113

- •CONE OF SILENCE –SECTION 2-486
- •PROTEST PROCEDURES –CODE SECTION 2-371
- •DEBARMENT PROCEEDINGS –SECTIONS 2-397 THROUGH 2-485.3
- •LOBBYIST REGISTRATION AND DISCLOSURE OF FEES – SECTIONS 2-481 THROUGH 2-406
- •CAMPAIGN CONTRIBUTIONS BY VENDORS – SECTION 2-487
- •CAMPAIGN CONTRIBUTIONS – SECTION 2-488
- •EQUAL BENEFITS FOR DOMESTIC PARTNERS – SECTION 2-373
- •~~LIVING WAGE REQUIREMENT – SECTIONS 2-407 THROUGH 2-410~~
- •FALSE CLAIMS ORDINANCE – SECTION 70-300
- •ACCEPTANCE OF GIFTS, FAVORS & SERVICES – SECTION 2-449

2. PUBLIC ENTITY CRIME. A person or affiliate who has been placed on the convicted vendor list following a conviction for public entity crimes may not submit a proposal on a contract to provide any goods or services to a public entity, may not submit a proposal on a contract with a public entity for the construction or repair of a public building or public work, may not submit a proposal on leases of real property to public entity, may not be awarded or perform work as a contractor, supplier, sub-contractor, or consultant under a contract with a public entity, and may not transact business with any public entity in excess of the threshold amount provided in Sec. 287.017, for CATEGORY TWO for a period of 36 months from the date of being placed on the convicted vendor list.

3. COMPLIANCE WITH THE CITY'S LOBBYIST LAWS. This RFQ is subject to, and all Proposers are expected to be or become familiar with, all City lobbyist laws. Proposers shall be solely responsible for ensuring that all City lobbyist laws are complied with, and shall be subject to any and all sanctions, as prescribed therein, including, without limitation, disqualification of their responses, in the event of such non-compliance.

4. DEBARMENT ORDINANCE: This RFQ is subject to, and all proposers are expected to be or become familiar with, the City's Debarment Ordinance as codified in Sections 2-397 through 2-406 of the City Code.

5. COMPLIANCE WITH THE CITY'S CAMPAIGN FINANCE REFORM LAWS. This RFQ is subject to, and all Proposers are expected to be or become familiar with, the City's Campaign Finance Reform laws, as codified in Sections 2-487 through 2-490 of the City Code. Proposers shall be solely responsible for ensuring that all applicable provisions of the City's Campaign Finance Reform laws are complied with, and shall be subject to any and all sanctions, as prescribed therein, including disqualification of their responses, in the event of such non-compliance.

6. CODE OF BUSINESS ETHICS. Pursuant to City Resolution No.2000-37379, the Proposer shall adopt a Code of Business Ethics ("Code") and submit that Code to the Procurement Division with its response or within five (5) days upon receipt of request. The Code shall, at a minimum, require the Proposer, to comply with all applicable governmental rules and regulations including, among others, the conflict of interest, lobbying and ethics provision of the City of Miami Beach and Miami Dade County.

7. AMERICANS WITH DISABILITIES ACT (ADA). Call 305-673-7490 to request material in accessible format; sign language interpreters (five (5) days in advance when possible), or information on access for persons with disabilities. For more information on ADA compliance, please call the Public Works Department, at 305-673- 7000, Extension 2984.

8. POSTPONEMENT OF DUE DATE FOR RECEIPT OF PROPOSALS. The City reserves the right to postpone the deadline for submittal of proposals and will make a reasonable effort to give at least three (3) calendar days written notice of any such postponement to all prospective Proposers through *BidSync*.

9. PROTESTS. Proposers that are not selected may protest any recommendation for selection of award in accordance with the proceedings established pursuant to the City's bid protest procedures, as codified in Sections 2-370 and 2-371 of the City Code (the City's Bid Protest Ordinance). Protest not timely made pursuant to the requirements of the City's Bid Protest Ordinance shall be barred.

10. JOINT VENTURES / SINGLE PURPOSE ENTITY. Joint Ventures are not allowed. Proposals shall be submitted only by the prime contractor. Proposals may, however, identify other sub-contractors or sub-consultants to the prime Proposer who may serve as team members.

11. VETERAN BUSINESS ENTERPRISES PREFERENCE. Pursuant to City Code Section 2-374, the City shall give a preference to a responsive and responsible Proposer which is a small business concern owned and controlled by a veteran(s) or which is a service-disabled veteran business enterprise, and which is within five percent (5%) of the lowest responsive, responsible proposer, by providing such proposer an opportunity of providing said goods or contractual services for the lowest responsive proposal amount (or in this RFQ, the highest proposal amount). Whenever, as a result of the foregoing preference, the adjusted prices of two (2) or more proposers which are a small business concern owned and controlled by a veteran(s) or a service-disabled veteran business enterprise constitute the lowest proposal pursuant to an RFQ or oral or written request for quotation, and such proposals are responsive, responsible and otherwise equal with respect to quality and service, then the award shall be made to the service-disabled veteran business enterprise.

12. AGREEMENT BY BIDDERS. Any individual that submits a proposal in response to this solicitation agrees to the following:

Any action taken by the City in response to Proposals made pursuant to this solicitation, or in making any award, or in failing or refusing to make any award pursuant to such Proposals, or in cancelling awards, or in withdrawing or cancelling this solicitation, either before or after issuance of an award, shall be without any liability or obligation on the part of the City.

The City may, at its sole and absolute discretion, reject any and all, or parts of any and all, responses; re-advertise this RFQ; postpone or cancel, at any time, this RFQ process; or waive any irregularities in this RFQ, or in any responses received as a result of this RFQ.

Reasonable efforts will be made to either award the proposer the contract or reject all proposals within one-hundred twenty (120) calendar days after proposal opening date. In accordance with Section 47 below, a Proposer may withdraw its proposal after expiration of one hundred twenty (120) calendar days from the date of proposal opening, by delivering written notice of withdrawal to the Procurement Department.

13. COSTS INCURRED BY PROPOSERS. All expenses involved with the preparation and submission of Proposals, or any work performed in connection therewith, shall be the sole responsibility (and shall be at the sole cost and expense) of the Proposer, and shall not be reimbursed by the City.

14. RELATIONSHIP TO THE CITY. It is the intent of the City, and Proposers hereby acknowledge and agree, that the successful Proposer is considered to be an independent contractor, and that neither the Proposer, nor the Proposer's employees, agents, and/or contractors, shall, under any circumstances, be considered employees or agents of the City.

15. OCCUPATIONAL HEALTH AND SAFETY. In compliance with Chapter 442, Florida Statutes, any toxic substance listed in Section 38F-41.03 of the Florida Administrative Code delivered as a result of this proposal must be accompanied by a Material Safety Data Sheet (MSDS) which may be obtained from the manufacturer.

16. ENVIRONMENTAL REGULATIONS. The City reserves the right to consider a Proposer's history of citations and/or violations of environmental regulations in investigating a Proposer's responsibility, and further reserves the right to declare a Proposer not responsible if the history of violations warrants such determination in the opinion of the City. Proposer shall submit with its proposal, a complete history of all citations and/or violations, notices and dispositions thereof. The non-submission of any such documentation shall be deemed to be an affirmation by the Proposer that there are no citations or violations. Proposer shall notify the City immediately of notice of any citation or violation which proposer may receive after the proposal opening date and during the time of performance of any contract awarded to it.

17. TAXES. The City of Miami Beach is exempt from all Federal Excise and State taxes.

18. MISTAKES. Proposers are expected to examine the terms, conditions, specifications, delivery schedules, proposed pricing, and all instructions pertaining to the goods and services relative to this RFQ. Failure to do so will be at the Proposer's risk and may result in the Proposal being non-responsive.

19. PAYMENT. Payment will be made by the City after the goods or services have been received, inspected, and found to comply with contract, specifications, free of damage or defect, and are properly invoiced. Invoices must be consistent with Purchase Order format.

20. COPYRIGHT, PATENTS & ROYALTIES. Proposer shall indemnify and save harmless the City of Miami Beach, Florida, and its officers, employees, contractors, and/or agents, from liability of any nature or kind, including cost and expenses for, or on account of, any copyrighted, patented, or unpatented invention, process, or article manufactured or used in the performance of the contract, including its use by the City of Miami Beach, Florida. If the Proposer uses any design, device or materials covered by letters, patent, or copyright, it is mutually understood and agreed, without exception, that the proposal prices shall include all royalties or cost arising from the use of such design, device, or materials in any way involved in the work.

21. DEFAULT. Failure or refusal of the successful Proposer to execute a contract following approval of such contract by the City Commission, or untimely withdrawal of a proposal response before such award is made and approved, may result in a claim for damages by the City, and may be grounds for removing the Proposer from the City's vendor list.

22. MANNER OF PERFORMANCE. Proposer agrees to perform its duties and obligations in a professional manner and in accordance with all applicable Local, State, County, and Federal laws, rules, regulations and codes. Lack of knowledge or ignorance by the Proposer with/of applicable laws will in no way be a cause for relief from responsibility. Proposer agrees that the work and services provided shall be provided by employees that are educated, trained, experienced, certified, and licensed in all areas encompassed within their designated duties. Proposer agrees to furnish to the City any and all documentation, certification, authorization, license, permit, or registration currently required by applicable laws, rules, and regulations. Proposer further certifies that it and its employees will keep all licenses, permits, registrations, authorizations, or certifications required by applicable laws or regulations in full force and effect during the term of this contract. Failure of Proposer to comply with this paragraph shall constitute a material breach of this contract.

Where Developer is required to enter or go on to City of Miami Beach property to deliver materials or perform work or services as a result of any contract resulting from this solicitation, the Developer will assume the full duty, obligation and expense of obtaining all necessary licenses, permits, and insurance, and assure all work complies with all applicable laws. The Developer shall be liable for any damages or loss to the City occasioned by negligence of the Developer, or its officers, employees, contractors, and/or agents, for failure to comply with applicable laws.

23. SPECIAL CONDITIONS. Any and all Special Conditions that may vary from these General Terms and Conditions shall have precedence.

24. NON-DISCRIMINATION. The Proposer certifies that it is in compliance with the non-discrimination clause contained in Section 202, Executive Order 11246, as amended by Executive Order 11375, relative to equal employment opportunity for all persons without regard to race, color, religion, sex or national origin. In accordance with the City's Human Rights Ordinance, codified in Chapter 62 of the City Code, Proposer shall prohibit discrimination by reason of race, color, national origin, religion, sex, intersexuality, gender identity, sexual orientation, disability, marital and familial status, age, ancestry, height, weight, domestic partner status, labor organization membership, familial situation, and political affiliation.

25. DEMONSTRATION OF COMPETENCY. The City may consider any evidence available regarding the financial, technical, and other qualifications and abilities of a Proposer, including past performance (experience) in making an award that is in the best interest of the City, including:

A. Pre-award inspection of the Proposer's facility may be made prior to the award of contract.
B. Proposals will only be considered from firms which are regularly engaged in the business of providing the goods and/or services as described in this solicitation.
C. Proposers must be able to demonstrate a good record of performance for a reasonable period of time, and have sufficient financial capacity, equipment, and organization to ensure that they can satisfactorily perform the services if awarded a contract under the terms and conditions of this solicitation.
D. The terms "equipment and organization", as used herein shall, be construed to mean a fully-equipped and well-established company in line with the best business practices in the industry, and as determined by the City.
E. The City may consider any evidence available regarding the financial, technical, and other qualifications and abilities of a Proposer, including past performance (experience), in making an award that is in the best interest of the City.
F. The City may require Proposer to show proof that it has been designated as authorized representatives of a manufacturer or supplier, which is the actual source of supply. In these instances, the City may also require material information from the source of supply regarding the quality, packaging, and characteristics of the products to be supply to the City.

26. ASSIGNMENT. The successful Proposer shall not assign, transfer, convey, sublet or otherwise dispose of the contract, including any or all of its right, title or interest therein, or his/her or its power to execute such contract, to any person, company or corporation, without the prior written consent of the City.

27. LAWS, PERMITS AND REGULATIONS. The Proposer shall obtain and pay for all licenses, permits, and inspection fees required to complete the work and shall comply with all applicable laws.

28. OPTIONAL CONTRACT USAGE. When the successful Proposer is in agreement, other units of government or non-profit agencies may participate in purchases pursuant to the award of this contract at the option of the unit of

government or non-profit agency.

29. VOLUME OF WORK. To the extent applicable, it is the intent of the City to purchase the goods and services specifically listed in this solicitation. However, the City reserves the right to purchase any goods or services awarded from State or other governmental contracts, or on an as-needed basis through the City's spot market purchase provisions.

30. DISPUTES. In the event of a conflict between the documents, the order of priority of the documents shall be as follows:

A. Any contract or agreement resulting from the award of this solicitation; then

B. Addendum issued for this solicitation, with the latest Addendum taking precedence; then

C. The solicitation; then

D. The Proposer's proposal in response to the solicitation.

31. INDEMNIFICATION. The Developer shall indemnify and hold harmless the City and its officers, employees, agents and instrumentalities from any and all liability, losses or damages, including attorney's fees and costs of defense, which the City or its officers, employees, agents or instrumentalities may incur as a result of claims, demands, suits, causes of actions or proceedings of any kind or nature arising out of, relating to or resulting from the performance of the agreement by the Developer or its employees, agents, servants, partners, principals or subcontractors. The Developer shall pay all claims and losses in connection therewith, and shall investigate and defend all claims, suits or actions of any kind or nature in the name of the City, where applicable, including appellate proceedings, and shall pay all costs, judgments, and attorney's fees which may be incurred thereon. The Developer expressly understands and agrees that any insurance protection required by any agreement with the City or otherwise provided by the Developer shall in no way limit the responsibility to indemnify, keep and save harmless and defend the City or its officers, employees, agents and instrumentalities as herein provided. The above indemnification provisions shall survive the expiration or termination of this Agreement.

32. FLORIDA PUBLIC RECORDS LAW. Proposers are hereby notified that all Proposals including, without limitation, any and all information and documentation submitted therewith, are exempt from public records requirements under Section 119.07(1), Florida Statutes, and s. 24(a), Art. 1 of the State Constitution until such time as the City provides notice of an intended decision or until thirty (30) days after opening of the proposals, whichever is earlier. Additionally, Developer agrees to be in full compliance with Florida Statute 119.0701 including, but not limited to, agreement to (a) Keep and maintain public records that ordinarily and necessarily would be required by the public agency in order to perform the services; (b) provide the public with access to public records on the same terms and conditions that the public agency would provide the records and at a cost that does not exceed the cost provided in this chapter or as otherwise provided by law; (c) Ensure that public records that are exempt or confidential and exempt from public records disclosure requirements are not disclosed except as authorized by law; (d) Meet all requirements for retaining public records and transfer, at no cost, to the public agency all public records in possession of the Developer upon termination of the contract and destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. All records stored electronically must be provided to the public agency in a format that is compatible with the information technology systems of the public agency.

33. OBSERVANCE OF LAWS. Proposers are expected to be familiar with, and comply with, all Federal, State,
County, and City laws, ordinances, codes, rules and regulations, and all orders and decrees of bodies or tribunals having jurisdiction or authority which, in any manner, may affect the scope of services and/or project contemplated by this RFQ (including, without limitation, the Americans with Disabilities Act, Title VII of the Civil Rights Act, the EEOC Uniform Guidelines, and all EEO regulations and guidelines). Ignorance of the law(s) on the part of the Proposer will in no way relieve it from responsibility for compliance.

34. CONFLICT OF INTEREST. All Proposers must disclose, in their Proposal, the name(s) of any officer, director, agent, or immediate family member (spouse, parent, sibling, and child) who is also an employee of the City of Miami Beach. Further, all Proposers must disclose the name of any City employee who owns, either directly or indirectly, an interest of ten (10%) percent or more in the Proposer entity or any of its affiliates.

35. MODIFICATION/WITHDRAWALS OF PROPOSALS. A Proposer may submit a modified Proposal to replace all or any portion of a previously submitted Proposal up until the Proposal due date and time. Modifications received after the Proposal due date and time will not be considered. Proposals shall be irrevocable until contract award unless withdrawn in writing prior to the Proposal due date, or after expiration of **120** calendar days from the opening of Proposals without a contract award. Letters of withdrawal received after the Proposal due date and before said expiration date, and letters of withdrawal received after contract award will not be considered.

36. EXCEPTIONS TO RFQ. Proposers must clearly indicate any exceptions they wish to take to any of the terms in this RFQ, and outline what, if any, alternative is being offered. All exceptions and alternatives shall be included and clearly delineated, in writing, in the Proposal. The City, at its sole and absolute discretion, may accept or reject any or all exceptions and alternatives. In cases in which exceptions and alternatives are rejected, the City shall require the Proposer to comply with the particular term and/or condition of the RFQ to which Proposer took exception to (as said term and/or condition was originally set forth in the RFQ and any exhibits or Addenda thereto).

37. ACCEPTANCE OF GIFTS, FAVORS, SERVICES. Proposers shall not offer any gratuities, favors, or anything of monetary value to any official, employee, or agent of the City, for the purpose of influencing consideration of this Proposal. Pursuant to Sec. 2-449 of the City Code, no officer or employee of the City shall accept any gift, favor or service that might reasonably tend improperly to influence him in the discharge of his official duties.

38. SUPPLEMENTAL INFORMATION. City reserves the right to request supplemental information from Proposers at any time during the RFQ solicitation process, unless otherwise noted herein.

SECTION 0300 PROPOSAL SUBMITTAL INSTRUCTIONS AND FORMAT

1. SEALED PROPOSALS. One original Proposal (preferably in 3-ring binder) must be submitted in an opaque, sealed envelope or container on or before the due date established for the receipt of proposals. Additionally, ten (10) bound copies and one (1) electronic format (CD or USB format) are to be submitted. The following information should be clearly marked on the face of the envelope or container in which the proposal is submitted: solicitation number, solicitation title, Proposer name, Proposer return address. Proposals received electronically, either through email or facsimile, are not acceptable and will be rejected.

2. LATE PROPOSALS. Proposals are to be received on or before the due date established herein. **Any Proposal received after the deadline established for receipt of Proposals will be considered late and not be accepted or will be returned to Proposer unopened.** The City does not accept responsibility for any delays, natural or otherwise.

3. NON-RESPONSIVENESS. Failure to comply with the following requirements shall result in a determination of non-responsiveness. Non-responsive proposals will not be considered.

1. Failure to submit a signed copy of Appendix A.
2. Failure to comply with the Minimum Eligibility Requirements (See Appendix C, Section 1).

4. OMITTED OR ADDITIONAL INFORMATION. With exception of the Proposal Certification Form (Appendix A-1) and the Cost Proposal, if applicable, the City reserves the right to seek any omitted information/documentation or any additional information from Proposer or other source(s), including but not limited to: any firm or principal information, applicable licensure, resumes of relevant individuals, client information, financial information, or any information the City deems necessary to evaluate the capacity of the Proposer to perform in accordance with contract requirements. Failure to submit any omitted or additional information in accordance with the City's request shall result in proposal being deemed non-responsive.

5. PROPOSAL FORMAT. In order to maintain comparability, facilitate the review process and assist the Evaluation Committee in review of Proposals, it is strongly recommended that Proposals be organized and tabbed in accordance with the sections and manner specified below. Hard copy submittal should be tabbed as enumerated below and contain a table of contents with page references. Electronic copies should also be tabbed and contain a table of contents with page references. Proposals that do not include the required information will be deemed non-responsive and will not be considered.

TAB 1	Cover Letter & Appendix A-1 and A-2

1.1 Cover Letter and Table of Contents. The cover letter must indicate Proposer and Proposer Primary Contact for the purposes of this solicitation.

1.2 Proposal Certification Form (Appendix A-1). Failure to submit the Proposal Certification Form with the Proposal shall result in Proposal being deemed non-responsive.

1.3 Questionnaire & Requirements Affidavit (Appendix A-2). Failure to submit the Questionnaire and Requirements Affidavit with the Proposal or as requested by the City shall result in Proposal being deemed non-responsive.

1.4 Appendix F System Requirements Matrix. Failure to submit the System Requirements Matrix with the Proposal or as requested by the City shall result in Proposal being deemed non-responsive.

TAB 2 Project Team Qualifications

2.1 Organizational Chart: An organizational chart depicting the structure and lines of authority and communication for all firms, principals and personnel involved in the project. Include information that describes the intended structure regarding project management, accountability and compliance with the terms of the RFQ.

2.2 Relevant Experience of Prime Proposer (Access Control System): Summarize projects where the Proposer and/or its principals have provided services similar to those described herein. For each project provide the following:

a. project name and scope of services provided;
b. client(s);
c. client(s) project manager and contact information;
d. contract value; and
e. term of the engagement.

2.3 List of Authorized Integrators/Installers (if applicable):

Provide a list of all Integrators/Installers authorized to provide integration/installation services for the proposed access control software system. For each Integrators/Installers provide the following:

a. firm's name;
b. installation/integration competencies, if applicable;
c. address;
d. email and phone number(s) of firm; and
e. project manager(s) or representative(s) and contact information.

2.4 List of Authorized Subcontractor(s) (if applicable):

Provide a list of all subcontractors authorized to provide integration/installation services for the proposed access control software system. For each subcontractor(s) provide the following:

a. subcontractor name;
b. subcontractor's competencies;
c. address and email and phone number(s) of subcontractor(s).

TAB 3 Software and Equipment Functionality

Submit detailed information on the software and equipment proposed, with a focus on the following, at a minimum, the following.

a. Describe the functionality of the software proposed, its capabilities and unique aspects when comparing market competition.
b. Describe software's integrability to other systems the City supports.
c. Describe software's interoperability with Window's active directory.
d. Describe software's backwards compatibility and/or interface to current Millenium software.
e. Describe software's backwards compatibility and/or interface to X-Protect software.
f. Describe hardware options and recommended manufacturers and suppliers.
g. Describe options and approaches available to the City of Miami Beach, given its unique challenges including its public safety departments, vast number of City facilities, and multi-level user types.

TAB 4	Approach and Methodology

Submit detailed information on the approach and methodology that the Proposer and its team has used in past in engagements in providing the services described herein with a focus on the following, at a minimum, the following.

a. Describe successful past experiences to conducting security assessments of clients in order to determine best practice approaches to implementing a new access control system.
b. Describe firm's process for preparing for emergency events and unforeseen events, such as power failures; data disruption, and critical failures.
c. Describe a typical project plan for a client such as Miami Beach, related timelines, and go-live process.

TAB 5	Installation & Maintenance

Submit detailed information on the approach and methodology that the Proposer and its team has used in past in engagements in providing the services described herein with a focus on the following, at a minimum, the following.

a. Describe the Proposer's distribution and installation channels for assuring that the City is only working with authorized integrators/installers, including a list of current authorized partner integrators/installers.
b. Describe the proposed maintenance, updating or upgrade programs to make sure that the selected system is always functional and up to date.
c. Describe available training and ongoing technical support that will be provided to the City and its users.
d. Describe a typical project plan for a client such as Miami Beach, including phases, related timelines, and go-live process.

Note: After Proposal submittal, the City reserves the right to require additional information from Proposers (or Proposer team members or sub-consultants) to determine: qualifications (including, but not limited to, litigation history, regulatory action, or additional references); and financial capability (including, but not limited to, annual reviewed/audited financial statements with the auditors notes for each of their last two complete fiscal years).

SECTION 0400 PROPOSAL EVALUATION

1. EVALUATION OF PROPOSALS. All responsive proposals will be evaluated in accordance with this section. If more than one proposal is received, the City Manager may appoint an Evaluation Committee to consider and provide feedback on the qualitative factors of each proposal. In the event that only one responsive proposal is received, the City Manager, after determination that the sole responsive proposal materially meets the requirements of the RFQ, may, without an evaluation committee, recommend to the City Commission that the Administration enter into negotiations. In the evaluation of proposals, Proposers may be requested to make additional written submissions of a clarifying nature or oral presentations to the Evaluation Committee. Failure to provide the requested information within the time prescribed may result in the disqualification of proposal.

2. QUALITATIVE FACTORS. The Evaluation Committee shall not consider quantitative factors (e.g., cost, veteran's preference, prior volume of work received) in its review of proposals. The Evaluation Committee shall act solely in an advisory capacity to the City Manager. The results of the Evaluation Committee process do not constitute an award recommendation. The City Manager may utilize, but is not bound by, the results of the Evaluation Committee process, as well as consider any feedback or information provided by staff, consultants or any other third-party in developing an award recommendation in accordance with Sub-section 3 below. In its review of proposals received, the Evaluation Committee may review and score all proposals, with or without conducting interview sessions, in accordance with the following criteria.

Qualitative Criteria	Maximum Points
Project Team Qualifications	30
Software and Equipment Functionality	30
Approach and Methodology	20
Installation and Maintenance	20
TOTAL AVAILABLE POINTS	**100**

3. QUANTITATIVE CRITERIA. To the results of the Evaluation Committee review and scoring of proposals as stipulated above, staff may award an extra five points to the any proposer to which the veteran's preference is applicable. See Section 0100, Sub-Section 10.

Quantitative Criteria	Maximum Points
Veterans Preference	5
TOTAL AVAILABLE STEP 2 POINTS	**5**

4. COST. Cost shall not be considered by the Evaluation Committee. Cost will only be considered by the City Manager in preparing his recommendation to the City Commission. In considering cost, or any other factor, quantitative factors, the City Manager may consider any feedback or information provided by staff, consultants or any other third-party in developing an award recommendation in accordance with Sub-section 5 below.

5. DETERMINATION OF AWARD. The City Manager shall consider qualitative and quantitative factors, in accordance with Sub-section 2 and 3 above, as well as any other factors he deems appropriate, to prepare the award recommendation for the proposer(s) he deems to be in the best interest of the City, or may recommend rejection of all proposals. The City Manager's recommendation need not be consistent with the scoring results of the Evaluation Committee process, if applicable, and shall take into consideration Miami Beach City Code Section 2-369, including the following considerations:

(1) The ability, capacity and skill of the Proposer to perform the contract.

(2) Whether the Proposer can perform the contract within the time specified, without delay or interference.

(3) The character, integrity, reputation, judgment, experience and efficiency of the Proposer.

(4) The quality of performance of previous contracts.

(5) The previous and existing compliance by the Proposer with laws and ordinances relating to the contract.

The City Commission shall consider the City Manager's recommendation and may approve such recommendation. The City Commission may also, at its option, reject the City Manager's recommendation and select another Proposer(s) which it deems to be in the best interest of the City, or it may also reject all Proposals.

Balance of Page Intentionally Left Blank

APPENDIX A

MIAMIBEACH

Proposal Certification, Questionnaire & Requirements Affidavit

RFQ 2020-009-JC
Citywide Security Access Software System

PROCUREMENT DEPARTMENT
1755 Meridian Avenue, 3rd Floor
Miami Beach, Florida 33139

APPENDIX A1 - PROPOSAL CERTIFICATION FORM

This document is a **REQUIRED FORM** that must be submitted fully completed and executed.

FAILURE TO SUBMIT THE PROPOSAL CERTIFICATION FORM WITH ITS PROPOSAL SHALL RESULT IN THE PROPOSAL BEING DEEMED NON-RESPONSIVE.

Solicitation No: RFQ 2020-009-JC	Solicitation Title: Citywide Security Access System	
Procurement Contact: Jason Crouch	Tel: 305-673-7000 x26694	Email: jasoncrouch@miamibeachfl.gov

PROPOSER'S NAME:		
NO. OF YEARS IN BUSINESS:	NO. OF YEARS IN BUSINESS LOCALLY:	NO. OF EMPLOYEES:
OTHER NAME(S) PROPOSER HAS OPERATED UNDER IN THE LAST 10 YEARS:		
FIRM PRIMARY ADDRESS (HEADQUARTERS):		
CITY:		
STATE:	ZIP CODE:	
TELEPHONE NO.:		
TOLL FREE NO.:		
FAX NO.:		
FIRM LOCAL ADDRESS:		
CITY:		
STATE:	ZIP CODE:	
PRIMARY ACCOUNT REPRESENTATIVE FOR THIS ENGAGEMENT:		
ACCOUNT REP TELEPHONE NO.:		
ACCOUNT REP TOLL FREE NO.:		
ACCOUNT REP EMAIL:		
FEDERAL TAX IDENTIFICATION NO.:		

Except as stipulated in General Condition 36, Proposer agrees: to complete and unconditional acceptance of the terms and conditions of this document, inclusive of this solicitation, all specifications, attachments, exhibits and appendices and the contents of any Addenda released hereto; to be bound, at a minimum, to any and all specifications, terms and conditions contained herein or Addenda; that the Proposer has not divulged, discussed, or compared the proposal with other Proposals and has not colluded with any other proposer or party to any other proposal; that proposer acknowledges that all information contained herein is part of the public domain as defined by the State of Florida Sunshine and Public Records Laws; that all responses, data and information contained in the proposal are true and accurate.

Name of Proposer 's Authorized Representative:	Title of Proposer 's Authorized Representative:
Signature of Proposer 's Authorized Representative:	Date:

APPENDIX A2 - QUESTIONNAIRE AND REQUIREMENTS AFFIDAVIT FORM

The purpose of this Proposal Certification, Questionnaire and Requirements Affidavit Form is to inform prospective Proposers of certain solicitation and contractual requirements, and to collect necessary information from Proposers in order that certain portions of responsiveness, responsibility and other determining factors and compliance with requirements may be evaluated. Attach any requested information.

Name of Proposer 's Authorized Representative:	Title of Proposer 's Authorized Representative:
Signature of Proposer 's Authorized Representative:	Date:

1. **Veteran Owned Business.** Is Proposer claiming a veteran owned business status?

   ☐ YES ☐ NO

   SUBMITTAL REQUIREMENT: Proposers claiming veteran owned business status shall submit a documentation proving that firm is certified as a veteran-owned business or a service-disabled veteran owned business by the State of Florida or United States federal government, as required pursuant to ordinance 2011-3748.

2. **Conflict Of Interest.** All Proposers must disclose, in their Proposal, the name(s) of any officer, director, agent, or immediate family member (spouse, parent, sibling, and child) who is also an employee of the City of Miami Beach. Further, all Proposers must disclose the name of any City employee who owns, either directly or indirectly, an interest of ten (10%) percent or more in the Proposer entity or any of its affiliates.

   SUBMITTAL REQUIREMENT: Proposers must disclose the name(s) of any officer, director, agent, or immediate family member (spouse, parent, sibling, and child) who is also an employee of the City of Miami Beach. Proposers must also disclose the name of any City employee who owns, either directly or indirectly, an interest of ten (10%) percent or more in the Proposer entity or any of its affiliates

3. **References & Past Performance.** Proposer shall attach at least three (3) references for whom the Proposer has completed work similar in size and nature as the work referenced in solicitation.

   SUBMITTAL REQUIREMENT: For each reference submitted, the following information is required: 1) Firm Name, 2) Contact Individual Name & Title, 3) Address, 4) Telephone, 5) Contact's Email and 6) Narrative on Scope of Services Provided.

4. **Suspension, Debarment or Contract Cancellation.** Has Proposer ever been debarred, suspended or other legal violation, or had a contract cancelled due to non-performance by any public sector agency?

   ☐ YES ☐ NO

   SUBMITTAL REQUIREMENT: If answer to above is "YES," Proposer shall submit a statement detailing the reasons that led to action(s).

5. **Vendor Campaign Contributions.** Proposers are expected to be or become familiar with, the City's Campaign Finance Reform laws, as codified in Sections 2-487 through 2-490 of the City Code. Proposers shall be solely responsible for ensuring that all applicable provisions of the City's Campaign Finance Reform laws are complied with, and shall be subject to any and all sanctions, as prescribed therein, including disqualification of their Proposals, in the event of such non-compliance.

   SUBMITTAL REQUIREMENT: Submit the names of all individuals or entities (including your sub-consultants) with a controlling financial interest as defined in solicitation. For each individual or entity with a controlling financial interest indicate whether or not each individual or entity has contributed to the campaign either directly or indirectly, of a candidate who has been elected to the office of Mayor or City Commissioner for the City of Miami Beach.

6. **Code of Business Ethics.** Pursuant to City Resolution No.2000-23879, each person or entity that seeks to do business with the City shall adopt a Code of Business Ethics ("Code") and submit that Code to the Procurement Department with its proposal/response or within five (5) days upon receipt of request. The Code shall, at a minimum, require the Proposer, to comply with all applicable governmental rules and regulations including, among others, the conflict of interest, lobbying and ethics provision of the City of Miami Beach and Miami Dade County.

   SUBMITTAL REQUIREMENT: Proposer shall attach its Code of Business Ethics. In lieu of submitting Code of Business Ethics, Proposer may submit a statement indicating that it will adopt, as required in the ordinance, the City of Miami Beach Code of Ethics, available at http://www.miamibeachfl.gov/city-hall/procurement/procurement-related-ordinance-and-procedures/

7. **Living Wage.** Pursuant to Section 2-408 of the City of Miami Beach Code, as same may be amended from time to time, covered employees shall be paid the required living wage rates listed below:

1. Effective January 1, 2018, covered employees must be paid a living wage rate of no less than $11.62 per hour with health care benefits of at least $2.26 per hour, or a living wage rate of no less than $13.88 per hour without health care benefits.
2. Effective January 1, 2019, covered employees must be paid a living wage rate of no less than $11.70 per hour with health care benefits of at least $2.74 per hour, or a living wage rate of no less than $14.44 per hour without health care benefits.
3. Effective January 1, 2020, covered employees must be paid a living wage rate of no less than $11.78 per hour with health care benefits of at least $3.22 per hour, or a living wage rate of no less than$15.00 per hour without health care benefits.

The living wage rate and health care benefits rate may, by Resolution of the City Commission be indexed annually for inflation using the Consumer Price Index for all Urban Consumers (CPI-U) Miami/Ft. Lauderdale, issued by the U.S. Department of Labor's Bureau of Labor Statistics. Notwithstanding the preceding, no annual index shall exceed three percent (3%). The City may also, by resolution, elect not to index the living wage rate in any particular year, if it determines it would not be fiscally sound to implement same (in a particular year).

Proposers' failure to comply with this provision shall be deemed a material breach under this proposal, under which the City may, at its sole option, immediately deem said Proposer as non-responsive, and may further subject Proposer to additional penalties and fines, as provided in the City's Living Wage Ordinance, as amended. Further information on the Living Wage requirement is available at http://www.miamibeachfl.gov/city-hall/procurement/procurement-related-ordinance-and-procedures/

Any payroll request made by the City during the contract term shall be completed electronically via the City's electronic compliance portal, LCP Tracker (LCPTracker.net).

SUBMITTAL REQUIREMENT: Indicate below that Proposer agrees to the living wage requirement. Failure to agree shall result in proposal disqualification.

☐ YES ☐ NO

8. **Equal Benefits for Employees with Spouses and Employees with Domestic Partners.** When awarding competitively solicited contracts valued at over $100,000 whose contractors maintain 51 or more full time employees on their payrolls during 20 or more calendar work weeks, the Equal Benefits for Domestic Partners Ordinance 2005-3494 requires certain contractors doing business with the City of Miami Beach, who are awarded a contract pursuant to competitive proposals, to provide "Equal Benefits" to their employees with domestic partners, as they provide to employees with spouses. The Ordinance applies to all employees of a Contractor who work within the City limits of the City of Miami Beach, Florida; and the Contractor's employees located in the United States, but outside of the City of Miami Beach limits, who are directly performing work on the contract within the City of Miami Beach.

A. Does your company provide or offer access to any benefits to employees with spouses or to spouses of employees?

☐ YES ☐ NO

B. Does your company provide or offer access to any benefits to employees with (same or opposite sex) domestic partners* or to domestic partners of employees?

☐ YES ☐ NO

C. Please check all benefits that apply to your answers above and list in the "other" section any additional benefits not already specified. Note: some benefits are provided to employees because they have a spouse or domestic partner, such as bereavement leave; other benefits are provided directly to the spouse or domestic partner, such as medical insurance.

BENEFIT	Firm Provides for Employees with Spouses	Firm Provides for Employees with Domestic Partners	Firm does not Provide Benefit
Health			
Sick Leave			
Family Medical Leave			
Bereavement Leave			

If Proposer cannot offer a benefit to domestic partners because of reasons outside your control, (e.g., there are no insurance providers in your area willing to offer domestic partner coverage) you may be eligible for Reasonable Measures compliance. To comply on this basis, you must agree to pay a cash equivalent and submit a completed Reasonable Measures Application (attached) with all necessary documentation. Your Reasonable Measures Application will be reviewed for consideration by the City Manager, or his designee. Approval is not guaranteed and the City Manager's decision is final. Further information on the Equal Benefits requirement is available at http://www.miamibeachfl.gov/city-hall/procurement/procurement-related-ordinance-and-procedures/

9. **Public Entity Crimes.** Section 287.133(2)(a), Florida Statutes, as currently enacted or as amended from time to time, states that a person or affiliate who has been placed on the convicted vendor list following a conviction for a public entity crime may not submit a proposal, proposal, or reply on a contract to provide any goods or services to a public entity; may not submit a proposal, proposal, or reply on a contract with a public entity for the construction or repair of a public building or public work; may not submit proposals, proposals, or replies on leases of real property to a public entity; may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity; and may not transact business with any public entity in excess of the threshold amount provided in s. 287.017 for CATEGORY TWO for a period of 36 months following the date of being placed on the convicted vendor list.

SUBMITTAL REQUIREMENT: Proposer agrees to the requirements of Section 287.133, Florida Statutes, and certifies it has not been placed on convicted vendor list. Failure to agree shall result in proposal disqualification.

☐ YES ☐ NO

10. **Non-Discrimination.** Pursuant to City Ordinance No.2016-3990, the City shall not enter into a contract with a business unless the business represents that it does not and will not engage in a boycott as defined in Section 2-375(a) of the City Code, including the blacklisting, divesting from, or otherwise refusing to deal with a person or entity when such action is based on race, color, national origin, religion, sex, intersexuality, gender identity, sexual orientation, marital or familial status, age or disability.

SUBMITTAL REQUIREMENT: Proposer agrees it is and shall remain in full compliance with Section 2-375 of the City of Miami Beach City Code. Failure to agree shall result in proposal disqualification.

☐ YES ☐ NO

11. **Moratorium on Travel to and the Purchase of Goods or Services from North Carolina and Mississippi.** Pursuant to Resolution 2016-29375, the City of Miami Beach, Florida, prohibits official City travel to the states of North Carolina and Mississippi, as well as the purchase of goods or services sourced in North Carolina and Mississippi. Proposer shall agree that no travel shall occur on behalf of the City to North Carolina or Mississippi, nor shall any product or services it provides to the City be sourced from these states.

SUBMITTAL REQUIREMENT: Proposer agrees it is and shall remain in full compliance with Resolution 2016-29375. Failure to agree shall result in proposal disqualification.

☐ YES ☐ NO

12. **Fair Chance Requirement.** Pursuant to Section 2-376 of the City Code, the City shall not enter into any contract resulting from a competitive solicitation, unless the proposer certifies in writing that the business has adopted and employs written policies, practices, and standards that are consistent with the City's Fair Chance Ordinance, set forth in Article V of Chapter 62 of the City Code ("Fair Chance Ordinance"), and which, among other things, (i) prohibits City contractors, as an employer, from inquiring about an applicant's criminal history until the applicant is given a conditional offer of employment; (ii) prohibits advertising of employment positions with a statement that an individual with a criminal record may not apply for the position, and (iii) prohibits placing a statement on an employment application that a person with a criminal record may not apply for the position.

SUBMITTAL REQUIREMENT: Proposer certifies that it has adopted policies, practices and standards consistent with the City's Fair Chance Ordinance. Proposer agrees to provide the City with supporting documentation evidencing its compliance upon request. Proposer further agrees that any breach of the representations made herein shall constitute a material breach of contract, and shall entitle the City to the immediate termination for cause of the agreement, in addition to any damages that may be available at law and in equity. Failure to agree shall result in proposal disqualification.

☐ YES ☐ NO

13. **Acknowledgement of Addendum.** After issuance of solicitation, the City may release one or more addendum to the solicitation which may provide additional information to Proposers or alter solicitation requirements. The City will strive to reach every Proposer having received solicitation through the City's e-procurement system, BidSync.com. However, Proposers are solely responsible for assuring they have received any and all addendum issued pursuant to solicitation. This Acknowledgement of Addendum section certifies that the Proposer has received all addendum released by the City pursuant to this solicitation. Failure to obtain and acknowledge receipt of all addenda may result in proposal disqualification.

Initial to Confirm Receipt		Initial to Confirm Receipt		Initial to Confirm Receipt	
	Addendum 1		Addendum 6		Addendum 11
	Addendum 2		Addendum 7		Addendum 12
	Addendum 3		Addendum 8		Addendum 13
	Addendum 4		Addendum 9		Addendum 14
	Addendum 5		Addendum 10		Addendum 15

APPENDIX B

MIAMIBEACH

"No Bid" Form

RFQ 2020-009-JC
Citywide Security Access Software System

PROCUREMENT DEPARTMENT
1755 Meridian Avenue, 3rd Floor
Miami Beach, Florida 33139

Note: It is important for those vendors who have received notification of this solicitation but have decided not to respond, to complete and submit the attached "Statement of No Bid." The "Statement of No Bid" provides the City with information on how to improve the solicitation process. Failure to submit a "Statement of No Bid" may result in not being notified of future solicitations by the City.

Statement of No Bid

WE HAVE ELECTED NOT TO SUBMIT A PROPOSAL AT THIS TIME FOR REASON(S) CHECKED AND/OR INDICATED BELOW:

___ Workload does not allow us to proposal

___Insufficient time to respond

___ Specifications unclear or too restrictive

___ Unable to meet specifications

___Unable to meet service requirements

___Unable to meet insurance requirements

___Do not offer this product/service

___OTHER. (Please specify)

_____

_____

_____

We do __ do not __ want to be retained on your mailing list for future proposals of this type product and/or service.

Signature:_____

Title:_____

Legal Company Name:_____

Note: Failure to respond, either by submitting a proposal or this completed form, may result in your company being removed from our vendors list.

PLEASE RETURN TO:
CITY OF MIAMI BEACH
PROCUREMENT DEPARTMENT
ATTN: **JASON CROUCH**
RFQ #**2020-009-JC**
1755 MERIDIAN AVENUE, 3RD FLOOR
MIAMI BEACH, FL 33139

APPENDIX C

MIAMIBEACH

Specifications & Special Conditions

RFQ 2020-009-JC
Citywide Security Access Software System

PROCUREMENT DEPARTMENT
1755 Meridian Avenue, 3rd Floor
Miami Beach, Florida 33139

A. General Background.

Presently, the City of Miami Beach (the "City") currently operates a citywide physical access control security system (hereafter referred to as "the system"), including software and hardware, based on Millennium Group software, which includes the primary function of granting door and facilities entry access by way of approved card credentials, thereby limiting physical access to buildings, offices, rooms, personnel, and City assets, as well as establish access rights. The system will be hosted on virtual servers by the City of Miami Beach IT Department, with primary and backup locations. Migration of current City data is recommended but not required, as manual entry may ultimately be in the City's best interest. By way of this RFQ, the City intends to procure an access control system that is robust, and customizable in order to fully meet the needs of the City's security infrastructure. Additionally, the City will require routine maintenance and emergency services for the system.

Through this RFQ, it is the City's intent to accomplish the following goals:

1) Select a Citywide Security Access Control System (hardware, software, and maintenance): The selected access control system shall provide, including but not limited to, an infrastructure of connected card readers, credentialed users, door locks, control panels, and alarms. The selected access control system will be integrated citywide in order to provide secure electronic door access to various City facilities. In response to this RFQ, Prospective Proposers may submit Proposals outlining its qualifications for the City's desired access control system and services which include, but not limited to, the following: access control software, system planning and integration, administration, credential management, hardware, training, support, and ancillary product options, including video management and cloud storage;

2) Pursuant to the selected security access control system, the City may standardize the respective access control system; and

3) Following the standardization, the City may prequalify manufacturers and/or authorized contractors for future installation/integration or maintenance work.

B. SPECIFICATIONS.

SECTION I. SELECTION OF ACCESS CONTROL SOFTWARE SYSTEM

At a minimum, the City requires the following:

1.1 **MANUFACTURERS:**

A. Basis-of-Design Product: Subject to compliance with requirements, provide products by one of the manufacturers specified.

B. Acceptable Manufacturer:

1. Lenel, or approved alternate.

C. DESCRIPTION:

1. Security Access System: PC-based central and regional servers and field-installed controllers, connected by a high-speed electronic-data transmission network.
2. System Software: Based on Windows 64-bit, workstation operating system, server operating system, and application software. Software shall have the following capabilities:
3. Multiuser and multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations.
4. Graphical user interface to show pull-down menus and a menu-tree format that complies with interface guidelines of Microsoft Windows.
5. System license for the entire system including capability for future additions that are within the indicated system size limits specified in this Section.
6. Open-architecture system that allows importing and exporting of data and interfacing with other systems that are compatible with Microsoft Windows.
7. Password-protected operator login and access.

8. Open-database-connectivity compliant.

1.2 **PACS FIELD HARDWARE**

A. Physical Access Control System (PACS) Field Hardware. The PACS shall be equipped with the access control field hardware required to receive alarms and administer all access granted or denied decisions. All field hardware must be designed to meet UL 294 requirements. The PACS must be able to retrieve device serial numbers from all field hardware, excluding card readers and keypads. Depending on the configuration, the PACS hardware must be able to include any or all of the following components:

1. Intelligent Controllers
    a. Native network support and is scalable to 64 doors/openings.
    b. OSDP Protocol secure channel security for reader connectivity.
    c. On-board Ethernet port to connect to server-based access control hosts.
    d. Performs access control, alarm management and scheduled operations.
    e. 600,000 cardholder capacity
    f. Supports up to 1024 inputs and 1024 outputs.
    g. Manufacturer:
        (1) Lenel, or approved alternate.
2. Intelligent Controller w/ Extended Applications
    a. Supports a variety of extended features including High Assurance Credential Authentication.
    b. OSDP Protocol secure channel security for reader connectivity and extended applications.
    c. Direct hardware support for 2 doors/openings and can scale to 64 doors/openings.
    d. Performs access control, alarm management and scheduled operations.
    e. On-board Ethernet port to connect to server-based access control hosts.
    f. 2,000,000 cardholder capacity
    g. Supports up to 1024 inputs and 1024 outputs
    h. Manufacturer:
        (1) Lenel, or approved alternate.
3. Edge-capable Intelligent Controllers
    a. Expandable up to 8 downstream serial input/output modules and expandable up to 17 doors/openings.
    b. OSDP Protocol secure channel security for reader connectivity.
    c. POE+ capable.
    d. 240,000 cardholder capacity.
    e. Supports up to 130 inputs and 130 outputs.
    f. Manufacturer:
        (1) Lenel, or approved alternate.
4. Input Controller Module
    a. Provides 16 general purpose input circuits.
    b. Inputs can be set for normally open or normally closed.
    c. Inputs can be declared supervised or non-supervised.
    d. Manufacturer:
        (1) Lenel, or approved alternate.
5. Output Control Module
    a. Provides 16 general purpose outputs as Form C relay contacts.
    b. Individually configurable parameters that can be set for timing and for fail-safe versus fail secure modes.
    c. Manufacturer:
        (1) Lenel, or approved alternate.
6. Single Reader Interface Panel.
    a. RS-485 connected and can be clustered or distributed depending on the installation requirements.
    b. OSDP Protocol secure channel security for reader connectivity.
    c. Provides all I/O needed for single door control.

d. Manufacturer:
(1) Lenel , or approved alternate.

7. Dual Reader Interface Panel.
   a. Provides all I/O needed for controlling two doors with auxiliary point control and monitoring.
   b. RS-485 Connected.
   c. OSDP Protocol secure channel security for reader connectivity.
   d. Manufacturer:
      (1) Lenel, or approved alternate.

B. **NFPA 70, Class II control transformers, NRTL listed. UL, CUL, and CE listed power Supplies and Enclosures. Transformers and power supplies for security access-control system shall not be shared with any other system**.

1. With power supplies sufficient enough to power at voltage and frequency required for field devices and portal-control devices.
2. Data Line Problems: For periods of loss of communication with the access server, or when data transmission is degraded and generating continuous checksum errors, the controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.
3. Store up to 1,000 transactions during periods of communication loss between the controller and access-control devices for subsequent upload to the access server on restoration of communication.
4. Controller Power: NFPA 70, Class II power-supply transformer, with 12 or 24VDC secondary, backup battery and charger.
5. Backup Battery: Valve-regulated, recombinant-sealed, lead-acid battery; spill proof. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.
6. Backup Power-Supply Capacity: 90 min. of battery supply. Submit battery and charger calculations.
7. Power Monitoring: Provide manual, dynamic battery-load test, initiated and monitored at the control center; with automatic disconnection of the controller when battery voltage drops below controller limits. Report by using local controller-mounted digital displays and by communicating status to central server. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:
8. Trouble Alarm: Low battery.
9. Alarm: Loss of A/C Power.

1.3 OPERATION:

A. Security access system must use a single database for access-control and credential-creation functions.

B. Security access system must be capable of accessing Active Directory for credential-creation and functions.

C. **Controller based Processing:**

1. Access-control information, including time, date, valid codes, access levels, and similar data, shall be downloaded to controllers so each controller can make access-control decisions.
2. Intermediate controllers for access control are prohibited.
3. In the event that communications with the central server is lost, controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the access server.

D. **Number of Locations:**

1. Support at least 255 separate database controllers using a single communications server with combinations dial-up, or TCP/IP LAN connections to each Location.
2. Each controller shall have its own database and history.

E. **System Network Requirements:**

1. System components shall be interconnected and shall provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.
2. Communication shall not require operator initiation or response and shall return to normal after partial- or total-network interruption such as power loss or transient upset.
3. System shall automatically communicate failures to the operator and shall identify the communications link that has experienced a partial or total failure.

F. 1. Central server shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central server shall control system networks to interconnect all system components, including workstations and field-installed controllers.

G. System Response to Alarms:

1. Alarms shall be communicated at the central server within three second of the alarm occurring at a controller or at a device controlled by a local controller, and within 1 second if the alarm occurs at the central server.
2. Alarm and status changes shall be displayed within 1 second after receipt of data by the central server.
3. All graphics shall be displayed, including graphics-generated map displays, on the console monitor within five seconds of alarm receipt at the security console.
4. This response time must be maintained during system heavy load.

H. 1. False-Alarm Reduction: The design of the central server and controllers must contain features to reduce false alarms. Equipment and software shall comply with SIA CP-01.

I. Error Detection:

1. A message will be in error if one bit is received incorrectly.
2. Retransmit messages with detected errors.
3. Monitor the frequency of data transmission failure for display and logging.

J. Data Line Supervision: System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.

K. Door Hardware Interface:

1. Comply with hardware requirements for door hardware that is required to be monitored or controlled by the security access system.
2. Electrical characteristics of controllers shall match the signal and power requirements of door hardware.

1.4 APPLICATION SOFTWARE:

A. **System Software**: Based on 64-bit server and workstation operating system and application software.

1. Multiuser multitasking should allow independent activities and monitoring to occur simultaneously at different workstations.
2. Graphical user interface should show pull-down menus and a menu-tree format.
3. Capability for future additions within the indicated
4. system size limits.
5. Open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with operating system.
6. Password-protected operator login and access.

B. **Peer Server Control Software**: Miami Beach will deploy virtual servers for the PACS system at Primary and Backup locations along with regional locations. Must detect a failure of a central server and cause the other central server to assume control of all system functions without interruption of operation. Both central servers should have drivers to support this mode of operation with Microsoft clustering supported failover or approved equivalent.

1. Two database server architecture (primary and failover)
2. Two application/communication servers (primary and failover)
3. One regional server at Miami Beach Police Department building.

C. **Application Software**: Interface between the alarm annunciation and entry-control controllers to monitor sensors, operate displays, report alarms, generate reports, and help train system operators.

1. Reside at the central server, workstations, and controllers as required to perform specified functions.
2. Operate and manage peripheral devices.
3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files, including size and location of each sequential and random-ordered record.
4. Import custom icons into graphics to represent alarms and I/O devices.
5. Locally link I/O so that any I/O can link to any other I/O within the same Location without requiring interaction with the host PC. This operation will be at the controller.
6. Locally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation will be at the controller.
7. Messages from PC to controllers and controllers to controllers will be on a polled network that utilizes check summing and acknowledgment of each message. Communication should be automatically verified, buffered, and retransmitted if message is not acknowledged.
8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-controller communications methods by changing the polling frequency and the amount of time the system waits for a response.
9. Automatic and encrypted backups for database and history backups must be automatically stored at the central server and encrypted with a nine-character alphanumeric password that must be used to restore or read data contained in backup.
10. Operator audit trail for recording and reporting all changes made to database and system software.

D. **Workstation Software**:
1. User levels shall be individually customized by login credentials to allow or disallow operator access to program functions for each Location. There should be NO logins that are not a part of a User Role which is populated by Active Directory Users and Security groups.
2. Workstation event filtering shall allow user to define events and alarms that will be displayed at each workstation. If an alarm is unacknowledged (not handled by another workstation) for a preset amount of time, the alarm will automatically appear on the filtered workstation.

E. **Controller Software:**
1. Controllers shall operate as autonomous, intelligent processing units.
   a. Controllers shall make decisions about access control, alarm monitoring, linking functions, and door-locking schedules for their operation, independent of other system components.
   b. Controllers shall be part of a fully distributed (and routable) processing-control network.
   c. The portion of the database associated with a controller, and consisting of parameters, constraints, and the latest value or status of points connected to that controller, shall be maintained in the controller.
2. **The following functions shall be fully implemented and operational within each controller:**
   a. Monitoring inputs.
   b. Controlling outputs.
   c. Automatically reporting alarms to the central server.
   d. Reporting of sensor and output status to the central server on request.
   e. Maintaining real time, automatically updated by the central server at least once a day.
   f. Communicating with the central server.
   g. Diagnosing.
   h. Downloading and uploading data to and from the central server.
3. **Controller Operations at a Location:**
   a. Up to 64 controllers connected to RS-485 communications loop. Globally operating I/O linking and anti-pass back functions between controllers within the same Location without central-station or workstation intervention. Linking and anti-pass back shall remain fully functional within the same Location even when the central server or workstations are off-line.
   b. In the event of communication failure between the central server and a Location, there should be no degradation in operations at the controllers at that Location. Controllers at

each Location shall be connected to a memory buffer with a capacity to store up to 10,000 events; there shall be no loss of transactions in system history files until the buffer overflows.

c. Buffered events shall be handled in a first-in-first-out mode of operation.

4. **Individual Controller Operation:**

a. Controllers shall transmit alarms, status changes, and other data to the central server when communications circuits are operable. If communications are not available, controllers shall function in a stand-alone mode; operational data, including the status and alarm data normally transmitted to the central server, shall be stored for later transmission to the central server. Storage capacity for the latest 1,024 events shall be provided at each controller.

b. Controllers shall provide a response to card readers or keypad entries in less than 0.25 second, regardless of system size.

c. Controllers that are reset, or powered up from a nonpowered state, shall automatically request a parameter download and reboot to their proper working state. This shall happen without any operator intervention.

d. Initial Startup: When controllers are brought on-line, database parameters must be automatically downloaded to them. After initial download is completed, only database changes must be downloaded to each controller.

e. On failure for any reason, controllers must perform an orderly shutdown and force controller outputs to a predetermined failure-mode state, consistent with the failure modes shown and the associated control device.

f. After power is restored, following a power failure, startup software must initiate self-test diagnostic routines, after which controllers must resume normal operation.

g. After controller failure, if the database and application software are no longer resident, controllers must not restart but must remain in the failure mode until repaired. If database and application programs are resident, controllers must immediately resume operation. If not, software must be restored automatically from the central server.

5. **Communications Monitoring:**

a. System shall monitor and report status of RS-485 communications loop of each Location.

b. Communication status window shall display which controllers are currently communicating, a total count of missed polls in a user configurable time period, and which controller last missed a poll.

c. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM for each controller.

6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the central server at least once a day to ±10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.

F. **Server-to-Controller Communications:**

1. Central-server or workstation communications must use the following:
   a. TCP/IP LAN interface cards.
2. Communication Server-to-controller and controller-to-controller communications (TCP/IP) must use a polled-communication protocol that checks sum and acknowledges each message. All communications in this subparagraph shall be verified and buffered and retransmitted if not acknowledged.

G. **TCP/IP PC-to-Controller Communications:**

1. Communication software on the PC must supervise the PC-to-controller communications link.
2. Loss of communications to any controller should result in an alarm at all PCs running the communication software.
3. When communications are restored, all buffered events should automatically upload to the PC, and any database changes shall be automatically sent to the controller.

H. **Controller-to-Controller Communications:**

1. RS-485, two-wire duplex, point-to-point, regenerative (repeater) communications network methodology.
2. RS-485 communications signal must be regenerated at each controller.

I. **Database Downloads:**

1. All data transmissions from PCs to a Location, and between controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.
2. If a controller is reset for any reason, it should automatically request and receive a database download from the PC. The download should restore data stored at the controller to their normal working state and must take place with no operator intervention.
3. Software shall provide for setting downloads via dial-up connection to once per 24-hour period, with time selected by the operator.
4. Software shall provide for setting delays of database downloads for dial-up connections. Delays change the download from immediately to a delay ranging from one to 999 min.

J. **Operator Interface:**

1. Inputs in system must have two icon representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs, displayed icons should automatically change to the proper icon to display the current system state in real time. Icons should also display the input's state, whether armed or bypassed, and if the input is in the armed or bypassed state due to a schedule or a manual command.
3. Outputs in system should have two icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. Icons displaying status of the I/O points should be constantly updated to show their current real-time condition without prompting by the operator.
5. The operator should be able to scroll the list of I/Os and press the appropriate toolbar button, or right click, to command the system to perform the desired function.
6. Graphic maps or drawings containing inputs, outputs, and override groups should include the following:
    a. Database to import and store full-color maps or CAD drawings and allow for input, output, and override group icons to be placed on maps.
    b. Maps to provide real-time display animation and allow for control of points assigned to them.
    c. System to allow inputs, outputs, and override groups to be placed on different maps.
    d. Software to allow changing the order or priority in which maps will be displayed.
7. Override Groups Containing I/Os:
    a. System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.
    b. Icon shall change automatically to show the live summary status of points in that group.
    c. Override group icon shall provide a method to manually control or set to time-zone points in the group.
    d. Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.
8. Schedule Overrides of I/Os and Override Groups:
    a. To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.
    b. Each schedule shall be composed of a minimum of two dates with separate times for each date.
    c. The first time and date shall be assigned the override state that the point shall advance to when the time and date become current.

d. The second time and date shall be assigned the state that the point shall return to when the time and date become current.

9. Copy command in database must allow for like data to be copied and then edited for specific requirements, to reduce redundant data entry.

K. **Operator Access Control:**

1. Control operator access to system controls through five configurable password-protected operator levels. Master installer level (full rights), Administrator level (complete system usage), Shift Lead level, Operator, and user level. Administrator level should be able to change all access levels for the Shift Lead, operator, and user levels.
2. Three successive attempts by an operator to execute functions beyond their defined level during a 24-hour period must initiate a software tamper alarm.
3. The password must not be displayed or printed.
4. Each password must be definable and assignable for the following:
   a. Selected commands to be usable.
   b. Access to system software.
   c. Access to application software.
   d. Individual zones that are to be accessed.
   e. Access to database.

L. **Operator Commands:**

1. Command Input: Plain-language words and acronyms should allow operators to use the system without extensive training or data-processing backgrounds. System prompts should be a word, a phrase, or an acronym.
2. Command inputs should be acknowledged, and processing should start in not less than one second.
3. Tasks that are executed by operator's commands will include the following:
   a. Acknowledge Alarms: Used to acknowledge that the operator has observed the alarm message.
   b. Place Zone in Access: Used to remotely disable intrusion-alarm circuits emanating from a specific zone. System should be structured so that console operator cannot disable tamper circuits.
   c. Place Zone in Secure: Used to remotely activate intrusion-alarm circuits emanating from a specific zone.
   d. System Test: Allows the operator to initiate a system-wide operational test.
   e. Zone Test: Allows the operator to initiate an operational test for a specific zone.
   f. Print reports.
   g. Change Operator: Used for changing operators.
   h. Display Graphics: Used to show any graphic displays implemented in the system. Graphic displays should be completed within 20 seconds from time of operator command.
   i. Run system tests.
   j. Generate and format reports.

   k. Request help with the system operation.
      (1) Include in main menus.
      (2) Provide unique, descriptive, context-sensitive help for selections and functions with the press of one function key.
      (3) Provide navigation to specific topic from within the first help window.
      (4) Help should be accessible outside the application program.

   l. Entry-Control Commands:
      (1) Lock (secure) or unlock (open) each controlled entry and exit through time-zone programming.
      (2) Arm or disarm each monitored input through time-zone programming.
      (3) Enable or disable readers or keypads through time-zone programming.

(4) Enable or disable cards or codes per entry point through access-level programming.

4. Command Input Errors: Show operator input assistance when a command cannot be executed because of operator input errors. Assistance screen should use plain-language words and phrases to explain why the command cannot be executed. Error responses that require an operator to look up a code in a manual or other document are not acceptable. Conditions causing operator assistance messages include the following:
   a. Command entered is incorrect or incomplete.
   b. Operator is restricted from using that command.
   c. Command addresses a point that is disabled or out of service.
   d. Command addresses a point that does not exist.
   e. Command is outside the system's capacity.

M. Alarms:

1. **System Setup:**
   a. Assign manual and automatic responses to incoming-point status change or alarms.
   b. Automatically respond to input with a link to other inputs, outputs, or operator-response plans; unique sound files; and maps or images that graphically represent the point location.
   c. Minimum of sixty-character message field for each alarm.
   d. Operator-response-action messages should allow message length of at least 65,000 characters, with database storage capacity of up to 32,000 messages.
   e. Secondary messages should be assignable by the operator for printing to provide further information and should be editable by the operator.
   f. Allow 25 secondary messages with a field of four lines of 60 characters each.
   g. Store the most recent 1,000 alarms for recall by the operator using the report generator.
2. **Software Tamper:**
   a. Communicate a tamper alarm when unauthorized changes to system database files are attempted. Three consecutive unsuccessful attempts to log onto system should generate a software tamper alarm.
   b. Communicate a software tamper alarm when an operator or other individual makes three consecutive unsuccessful attempts to invoke functions beyond the authorization level.
   c. Maintain a transcript file of the last 5,000 commands entered at each central server to serve as an audit trail. System shouuld not allow write access to system transcript files by any person, regardless of their authorization level.
   d. Allow only acknowledgment of software tamper alarms.
3. Read access to system transcript files should be reserved for operators with the highest password authorization level available in system.
4. Animated Response Graphics: Highlight alarms with flashing icons on graphic maps; display and constantly update the current status of alarm inputs and outputs in real time through animated icons.
5. Multimedia Alarm Annunciation: Audio files to be associated with alarm events for audio annunciation or instructions.
6. Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, with options of requiring the operator to enter a comment about disposition of alarm. Allow operator to silence alarm sound when alarm is acknowledged.
7. Alarm Automation Interface: High-level interface to central-station alarm automation software systems. Allows input alarms to be passed to and handled by automation systems in the same manner as burglar alarms.
8. Video Surveillance Alarm Interface: Allow commands to be sent to video surveillance systems during alarms (or input change of state).
9. Camera Control: Provides operator ability to select and control cameras from graphic maps.

10. Alarm Monitoring: Monitor sensors, controllers, and notify operators of an alarm condition. Display higher-priority alarms first and, within alarm priorities, display the oldest unacknowledged alarm first. Operator acknowledgment of one alarm must not be considered acknowledgment of other alarms nor should it inhibit reporting of subsequent alarms.
11. Displayed alarm data should include type of alarm, location of alarm, and secondary alarm messages.
12. Maps should automatically display the alarm condition for each input assigned to that map if that option is selected for that input location.
13. Alarms initiate a status of "pending" and require the following two handling steps by operators:
    a. First Operator Step: "Acknowledged." This action should silence sounds associated with the alarm. The alarm remains in the system "Acknowledged" but "Un-Resolved."
    b. Second Operator Step: Operators enter the resolution or operator comment, giving the disposition of the alarm event. The alarm should then clear.
14. Each workstation should display the total pending alarms and total unresolved alarms.
15. Each alarm point should be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.
16. Alarms must transmit to the central server in real time except for allowing connection time for dial-up locations.
17. Alarms may be displayed and managed from different windows.
    a. Input Status: Overlay status icon with a large blinking icon.
    b. Alarm Window: Display name, time, and date in red.
    c. Graphic Map Display: Display a steady colored icon representing each alarm input location. Change icon to flashing red when the alarm occurs. Change icon from flashing red to steady red when the alarm is acknowledged.
18. Once an alarm is acknowledged, the operator must be prompted to enter comments about the nature of the alarm and actions taken. Operator's comments may be manually entered or selected from a programmed predefined list, or a combination of both.
19. For locations where there are regular alarm occurrences, provide programmed comments. Selecting that comment will clear the alarm.
20. The time and name of the operator who acknowledged and resolved the alarm must be recorded in the database.
21. Identical alarms from the same alarm point should be acknowledged at the same time the operator acknowledges the first alarm. Identical alarms must be resolved when the first alarm is resolved.
22. Alarm functions must have priority over downloading, retrieving, and updating database from workstations and controllers.
23. When a reader-controlled output (relay) is opened, the corresponding alarm point must be automatically bypassed.

N. Monitor Display: Display text and graphic maps that include zone status integrated into the display. Colors are used for the various components and current data. Colors should be uniform throughout the system.

1. Color Code:
    a. FLASHING RED: Alerts operator that a zone has gone into an alarm or that primary power has failed.
    b. STEADY RED: Alerts operator that a zone is in alarm and alarm has been acknowledged.
    c. YELLOW: Advises operator that a zone is in access.
    d. GREEN: Indicates that a zone is secure, and that power is on.

2. Graphics:
    a. Support 32,000 graphic display maps and allow import of maps from a minimum of 16 standard formats from another drawing or graphics program.
    b. Allow I/O to be placed on graphic maps by the drag-and-drop method.

c. Operators should be able to view the inputs, outputs, and the point's name by moving the mouse cursor over the point on the graphic map.
d. Inputs or outputs may be placed on multiple graphic maps. The operator should be able to toggle to view graphic maps associated with I/Os.
e. Each graphic map should have a display-order sequence number associated with it to provide a predetermined order when toggled to different views.
f. Camera icons should have the ability to be placed on graphic maps, when selected by an operator, will open a video window, display the camera associated with that icon, and provide pan-tilt-zoom control.
g. Input, output, or camera placed on a map should allow the ability to arm or bypass an input, open or secure an output, or control the pan-tilt-zoom function of the selected camera.
h. System test software will be a separate and isolated system for version updates, changes and patches to be utilized before inserting into the production system. It will be a mirror of the production database and associated panel/hardware types utilized in the production system

O. Reports:

1. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm (such as door alarm, intrusion alarm, tamper alarm, etc.), the type of sensor, the location, the time, and the action taken.
2. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.
3. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future recall.
4. Automatic History Reports: Named, saved, and scheduled for automatic generation.
5. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.
6. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.
7. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.
8. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain system installation data within system database so that data are available on-site at all times.
9. History Reports: Custom reports that allow the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.
    a. Initially store history on the server of the host PC.
    b. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.
    c. Each report shall depict the date, time, event type, event description, and device; or I/O name, cardholder group assignment, and cardholder name or code number.
    d. Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.
    e. Total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms," the total must reflect how many alarms occurred during that period.
10. Reports shall have the following four options:
    a. View on screen.
    b. Print. Include automatic print spooling and "Print To" options if more than one printer is connected to the system.
    c. "Save to File" with full path statement.
    d. System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that are abnormal, out of schedule, manually overridden, not reporting, or in alarm.

11. Custom Code List Subroutine: Allow the access codes of system to be sorted and printed according to the following criteria:
    a. Active, inactive, or future activate or deactivate.
    b. Code number, name, or imprinted card number.
    c. Group, Location access levels.
    d. Start and stop code range.
    e. Codes that have not been used since a selectablenumber of days.
    f. In, out, or either status.
    g. Codes with trace designation.

12. The reports of system database shall allow options so that every data field may be printed.
13. The reports of system database shall be constructed so that the actual position of the printed data shall closely match the position of the data on the data-entry windows.
14. Database management functions shall allow operators to add, delete, and modify access data as needed.
15. The enrollment station shall not have alarm response or acknowledgment functions.
16. Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.
17. The program shall provide means to disable the enrollment station when it is unattended, to prevent unauthorized use.
18. The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations. In the case of personnel identity-verification subsystems. Allow entry of personnel identifying information into the system database using menu selections and data fields. The data field names shall be customized during setup to suit user and site needs. Personnel identity-verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.
19. Cardholder Data: Provide 99 user-defined fields. System shall have the ability to run searches and reports using any combination of these fields. Each user-defined field shall be configurable, using any combination of the following features:
    a. MASK: Determines a specific format with which data must comply.
    b. REQUIRED: Operator is required to enter data into field before saving.
    c. UNIQUE: Data entered must be unique.
    d. DEACTIVATE DATE: Data entered will be evaluated as an additional deactivate date for all cards assigned to this cardholder.
    e. NAME ID: Data entered will be considered a unique ID for the cardholder.
20. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.
21. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.
22. Batch card printing.
23. Default card data can be programmed to speed data entry for sites where most card data are similar.
24. Enhanced ASCII File Import Utility: Allows the importing of cardholder data and images.
25. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.
26. Access Level expiration: Allow automated activation and deactivation of individual card, credential record, or access levels.
27. Test Report: The results of each test shall be stored for future display or printout. The report shall document the operational status of system components.
28. Report-Generator Software: Include commands to generate reports for displaying, printing, and storing on removable media. Reports shall be stored by type, date, and time. Report

printing shall be the lowest-priority activity. Report-generation mode shall be operator selectable but set up initially as periodic, automatic, or on request. Include time and date printed and the name of operator generating the report. Report formats may be configured by operators.

1.5 **SYSTEM DATABASE:**

A. **File Management:**

1. File management shall include database backup and restoration system, allowing selection of storage media, including CDR, DVD, or USB drive, and designated network resources.
2. Operations shall be both manual and automatic modes. The number of automatic sequential backups before the oldest backup will be overwritten; FIFO mode must be operator selectable.
3. Backup program shall provide manual operation from any PC on the LAN and shall operate while system remains operational.

B. **Access Card/Code Operation and Management**: Access authorization shall be by card, by a manually entered code (PIN), or by a combination of both (card plus PIN).

1. Access authorization shall verify the facility code first, the card or card-and-PIN validation second, and the access level (time of day, day of week, date), and number of uses last.
2. Use data-entry windows to view, edit, and issue access levels. Access-authorization entry-management system shall maintain and coordinate all access levels to prevent duplication or the incorrect creation of levels.
3. Allow assignment of multiple cards/codes to a cardholder.
4. Allow assignment of up to four access levels for each Location to a cardholder. Each access level may contain any combination of doors.
5. Each door may be assigned four distinct schedules.
6. Access codes may be up to 11 digits in length.
7. Software shall allow the grouping of locations to allow cardholder data to be shared by all locations in the group.
8. Cardholder Tracing: Allow for selection of cardholder for tracing. Make a special audible and visible annunciation at control station when a selected card or code is used at a designated code reader. Annunciation must include an automatic display of the cardholder image.
9. Allow each cardholder to be given either an unlimited number of uses or a number from one to 9,999 that regulates the number of times the card can be used before it is automatically deactivated.
10. Provide for cards and codes to be activated and deactivated manually or automatically by date. Provide for multiple deactivate dates to be preprogrammed.

C. **Security Access Integration**:

1. Photo ID badging and photo verification shall use the same database as the security access and may query data from cardholder, group, and other personal information to build a custom ID badge.
2. Automatic or manual image recall and manual access based on photo verification shall also be a means of access verification and entry.
3. System shall allow sorting of cardholders together by group or other characteristic for a fast and efficient method of reporting on, and enabling or disabling, cards or codes.

D. **Facility Codes:** System shall accommodate up to 2,048 facility codes per Location, with the option of allowing facility codes to work at all doors or only at particular doors.

E. **Operator Comments:**

1. With the press of one appropriate button on the toolbar, the user will be permitted to enter operator comments into the history at any time.
2. Automatic prompting of operator comment will occur before the resolution of each alarm.
3. Operator comments will be recorded by time, date, and operator number.
4. Comments will be sorted and viewed through reports and history.
5. The operator may enter comments in two ways; either or both may be used:

a. Manually entered through keyboard data entry (typed), up to 65,000 characters per each alarm.
b. Predefined and stored in database for retrieval on request.

6. System shall have a minimum of 999 predefined operator comments with up to 30 characters per comment.

F. Group:

1. Group names may be used to sort cardholders into groups that allow the operator to determine the tenant, vendor, contractor, department, division, or any other designation of a group to which the person belongs.
2. System software shall have the capacity to assign one of 32,000 group names to an access authorization.
3. Make provision in software to deactivate and reactivate all access authorizations assigned to a particular group.
4. Allow sorting of history reports and code list printouts by group name.

G. Schedules:

1. Each schedule consists of a start and stop time for seven days of the week and three holiday schedules. A schedule is assigned to inputs, outputs, or access levels to determine when an input will automatically arm or disarm, when an output automatically opens or secures, or when access authorization assigned to an access level will be denied or granted.
2. Up to four schedules may be assigned to inputs and outputs to allow up to four arm or disarm periods per day or four lock or unlock periods per day; up to three holiday override schedules may be assigned to a schedule.
3. Data-entry window will display a dynamically linked bar graph showing active and inactive times for each day and holiday, as start and stop times are entered or edited.
4. System shall have the capacity for 2,048 schedules for each Location.

H. Holidays:

1. Three different holiday schedules may be assigned to a schedule. Holiday schedule consists of date in format MM/DD/YYYY and a description. When the holiday date matches the current date of the schedule, the holiday schedule replaces the schedule for that 24-hour period.
2. System shall have the capacity for 255 annual holidays.
3. Three separate holiday schedules may be applied to a schedule.
4. Holidays have an option to be designated as occurring on the designated date each year. These holidays remain in the system and will not be purged.
5. Holidays not designated to occur each year must be automatically purged from the database after the date expires.

I. Access Levels:

1. System shall allow for the creation of up to 32,000 access levels.
2. One level must be predefined as the Master Access Level. The Master Access Level must work at all doors at all times and override any anti-pass back.
3. System shall allow for access to be restricted to any area by reader and by time. Access levels shall determine when and where an Identifier is authorized.
4. System shall be able to create multiple door and time-zone combinations under the same access level so that an Identifier may be valid during different time periods at different readers even if the readers are on the same controller.

J. User-Defined Fields:

1. System shall provide a minimum of 99 user-defined fields, each with up to 50 characters, for specific information about each credential holder.
2. System shall accommodate a title for each field; field length shall be 20 characters.
3. A "Required" option may be applied to each user-defined field that, when selected, forces the operator to enter data in the user-defined field before the credential can be saved.

4. A "Unique" option may be applied to each user-defined field that, when selected, will not allow duplicate data from different credential holders to be entered.
5. Data format option may be assigned to each user-defined field that will require the data to be entered with certain character types in specific spots in the field entry window.
6. A user-defined field, if selected, will define the field as a deactivate date. The selection must automatically cause the data to be formatted with the windows MM/DD/YYYY date format. The credential of the holder will be deactivated on that date.
7. A search function shall allow any one user-defined field or combination of user-defined fields to be searched to find the appropriate cardholder. The search function must include a search for a character string.
8. System shall have the ability to print cardholders based on and organized by the user-defined fields.

2.1 SUMMARY:

1. Provide Access Control equipment to replace the existing Millennium PACS
2. Access control system shall fully integrate with the City's current version of Milestone Video Management System.
3. Provide door hardware as shown on security design documents to bring existing doors up to code compliance.
4. Replace existing Millennium door controllers with Mercury based access controllers.
5. Replace all existing power supplies with Class 2 output rated power supplies.
6. Replace existing Indala card readers with HID SEOS multiCLASS card readers with the capability to support existing Indala credential technology and new SEOS credential technology.
7. Provide wiring, door contacts and request to exit devices per design documents for card reader doors and non-card reader exterior doors.
8. Provide HID SEOS credentials to cover all current card holders plus an additional 25%.
9. Migrate existing card holder data from Millennium database to new access control system database.
10. Integrate the new Access Control System with HR database.
11. Integrate the new Access Control System with Active Directory.
12. Provide graphical user interface which will include maps with interactive icons.

2.2 REFERENCE STANDARDS:

A. The references to the following code, references, and standards are meant to represent the most current and up-to-date revisions or printing as of the issue of this document. The Contractor is responsible for following the correct revision or printing.

B. Execute all Work in accordance with, and comply at a minimum with, National Fire Protection Association (NFPA) codes, state and local building codes, and all other applicable codes and ordinances in force, governing the particular class of work involved, for performance, workmanship, equipment, and materials. Where conflicts between various codes, ordinances, rules, and regulations exist, comply with the most stringent.

C. If the conflict is not reported timely, resolve the conflict and provide the installation in accordance with the governing codes and to the satisfaction of the Miami Beach site representative, without additional compensation. Contractor will be held responsible for any violation of the law.

D. Electronic Industries Alliance/Electronic Components, Assemblies & Materials Association (EIA/ECA):
   1. EIA/ECA-310-E - Cabinets, Racks, Panels, and Associated Equipment

E. The Institute of Electrical and Electronics Engineers, Inc. (IEEE):

1. IEEE 802.3 - Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (ANSI).
2. IEEE 1100 - Recommended Practice for Powering and Grounding Electronic Equipment (ANSI)

F. National Electrical Contractors Association (NECA):
    1. NECA 1 - Good Workmanship in Electrical Construction (ANSI)
G. National Electrical Manufacturers Association (NEMA):
    1. NEMA 250: Enclosures for Electrical Equipment (1000 Volts Maximum)
H. NFPA
    1. NFPA 70 - National Electrical Code.
    2. NFPA 101 – Life Safety Code.
    3. NFPA 262 - Test for Flame Travel and Smoke of Wires and Cables for Use in Air-Handling Spaces.
I. Telecommunications Industry Association (TIA):
    1. TIA 232-F - Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange.
    2. TIA 485-A - Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems.
    3. TIA 569-B - Commercial Building Standard for Telecommunications Pathways and Spaces Telecommunications Industry Association/Electronic Industries Alliance.
    4. TIA/EIA 568-B.1 - Commercial Building Telecommunications Cabling Standards - Part 1: General Requirements.
    5. TIA/EIA 606-A - Administration Standard for Commercial Telecommunications Infrastructure.
J. Underwriters Laboratories Inc.:
    1. UL 294 - Access Control System Units.
    2. UL 924 - Emergency Lighting and Power Equipment.
    3. UL 1581 - Electrical Wires, Cables, and Flexible Cords.
    4. UL 1666 - Test for Flame Propagation Height of Electrical and Optical-Fiber Cables Installed Vertically in Shafts.

K. Product Data: For each type of product indicated. Include rated capacities, operating characteristics, and furnished specialties and accessories. Reference each product to a location on Drawings. Test and evaluation data presented in Product Data must comply with SIA BIO-01.

L. Shop Drawings:
    1. Site and floor plans with device and equipment locations.
    2. Block diagrams of system component connections.
    3. Panel Elevations.
    4. Cable management system schedule where new cable is to be installed.
    5. Battery and load calculations for controllers and power supplies.
    6. Graphical maps for use on the monitor display showing equipment, device location and status.

M. Qualifications:
    1. Certificates for project manager and installer performing work.

N. Other Action Submittals:
    1. Project planning documents as specified in Part 3.

O. Field quality control reports.

P. Operation and Maintenance Data: For security system to include in emergency, operation, and maintenance manuals. In addition to items specified in Division 01, Section "Operation and Maintenance Data," include the following:
    1. Software documentation.
    2. Hard copies of manufacturer's specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on USB drive of the hard-copy submittal.
    3. System installation and setup guides with data forms to plan and record options and setup decisions.
    4. Provide hard copy printouts of wiring diagrams attached to inside door of each panel in a moisture resistant sleeve.
    5. Access control system training manuals (Admin and Operator Level)

Q. Furnish extra materials that match products installed and that are packaged with protective covering for storage and identified with labels describing contents.

1. Fuses of all kinds, power and electronic, equal to 10% of amount installed for each size used.
2. 10 of each type of Card Reader
3. 2 of each type controller

2.4 **QUALITY ASSURANCE**:

Installer Qualifications: An employer of workers trained and certified by manufacturer.

1. Project Manager that possesses one or more of the following:
   a. RCDD by Building Industry Consulting Service International (BICSI)
   b. Technology related degree from an ABET accredited institution.
2. Lead Installer Technician must be in good standing of the following:
   a. Dedicated 100% of their time on this project.
   b. BICSI certified level one commercial installer.
   c. Certified as an installer by each Manufacturer whose equipment and software are being installed on the project.
3. Minimum five (5) continuous years in the business of integrating and/or installing electronic safety and security systems.
4. Source Limitations: Obtain, controllers, card readers, and access control software through one source from single manufacturer.
5. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.
6. Comply with NFPA 70, "National Electrical Code."
7. Comply with NFPA 101, “Life Safety Code.”
8. Comply with SIA DC-01, SIA DC-03 and SIA DC-07.

2.5 **DELIVERY, STORAGE, AND HANDLING:**

A. Access Control Hardware:

1. Store in temperature- and humidity-controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85°F (10 and 30°C), and not more than 80% relative humidity, noncondensing.
2. Open each container; verify contents against packing list; and file copy of packing list, complete with container identification, for inclusion in operation and maintenance data.
3. Save original manufacturer's containers and packing materials and deliver as directed.

2.6 **PROJECT CONDITIONS:**

A. Environmental Conditions: System shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:

1. Control Station: Rated for continuous operation in ambient conditions of 60 to 85°F (16 to 30°C) and a relative humidity of 20 to 80%, noncondensing.
2. Indoor, Uncontrolled Environment: Type 3R enclosures. System components installed in non-air-conditioned, non-temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of [0 to 122°F (-18 to +50°C) dry bulb and 20 to 90% relative humidity, noncondensing.
3. Outdoor Environment: NEMA 250, NEMA 250, Type 4 enclosures. System components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions of -30 to +122°F (-34 to +50°C) and 20 to 90% relative humidity, condensing. Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to 85 mph (137 km/h) [and snow cover up to 24 inches (610 mm) thick].
4. Hazardous Environment: System components located in areas where fire or explosion hazards may exist because of flammable gases or vapors, flammable liquids, combustible dust, or ignitable fibers must be rated, listed, and installed according to NFPA 70.

2.7 CARD READER PRODUCT

1. HID multiCLASS SEOS OSDP credential readers:
   a. Wall-Mount Contactless Card Reader.
      (1) iClass SEOS Card format

(2) OSDP Reader Protocol
(3) 3.2" Reader Range
(4) Operating Voltage 5-16 VDC
(5) Standard Current draw 40 mA @ 16 VDC
(6) Peak Current draw 200 mA @ 16 VDC

b. Mullion-Mount Contactless Card Reader
(1) iClass SEOS Card format
(2) OSDP Reader Protocol
(3) 2.4" Reader Range
(4) Operating Voltage 5-16 VDC
(5) Standard Current draw 35 mA @ 16 VDC
(6) Peak Current draw 200 mA @ 16 VDC

c. Pedestal-Mount Contactless Card Reader
(1) iClass SEOS Card format
(2) OSDP Reader Protocol
(3) 4.7" Reader Range
(4) Operating Voltage 12 VDC o 24 VDC
(5) Standard Current draw 110 mA @ 12 VDC
(6) Peak Current draw 300 mA @ 12 VDC

2. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the controller. Response time shall be 800 ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.

3. Enclosure: Suitable for surface, semi-flush, pedestal, or weatherproof mounting. Mounting types must additionally be suitable for installation in the following locations:

a. Indoors, controlled environment.
b. Indoors, uncontrolled environment.
c. Outdoors, with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.

2.8 **TAMPER PROTECTION:**

A. Tamper Protection: Tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled. Control-station control-unit alarm display shall identify tamper alarms and indicate locations.

2.9 **ACCESS CONTROL HARDWARE:**

A. Access Control Client Computer provided by Miami Beach: The Client computer must meet the medium to high requirements of the Access Software's recommended client computer requirements.

B. Redundant Access Control Server with Microsoft clustering supported failover or equivalent: One identical redundant access control server computer, connected in a hot standby, peer configuration. This computer must automatically maintain its own copies of system software, application software, and data files. System transactions and other activities that alter system data files must be updated to system files of redundant computer in near real time. If primary access control computer fails, redundant access control computer must assume control immediately and automatically.

1. Two database server's architecture (primary and failover)
2. Two application/communications servers (primary and failover)
3. One physical application/communications for physical dial-up
4. One physical regional server at Miami Beach Police Department building.
5. With power supplies sufficient enough to power at voltage and frequency required for field devices and portal-control devices.
6. Data Line Problems: For periods of loss of communication with the access server, or when data transmission is degraded and generating continuous checksum errors, the controller must continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices. Store up to 1,000

transactions during periods of communication loss between the controller and access-control devices for subsequent upload to the access server on restoration of communication.

C. Badges and Credential Cards (HID SEOS 500x):
1. Badges are credential cards that do not contain data to be read by card readers.

2. Credential cards must store uniquely coded data used by card readers as an Identifier.
   a. Proximity Cards: Use proximity detection without physical contact with the reader for proper operation.
3. Allow entry-control card to be modified by lamination or direct print process during the enrollment process for use as a picture and identification badge without reduction of readability. The design shall allow for the addition of at least one slot or hole to accommodate the attachment of a clip for affixing the credential card to the type of badge holder used at the Site.

2.10 VIDEO AND CAMERA CONTROL

A. Control station or designated workstation displays live video from a video surveillance source.
1. Control Buttons: On the display window, with separate control buttons to represent Left, Right, Up, Down, Zoom In, Zoom Out, Scan, and a minimum of two custom-command auxiliary controls.
2. Provide at least seven icons to represent different types of cameras, with ability to import custom icons. Provide option for display of icons on graphic maps to represent their physical location.
3. Provide the alarm-handling window with a command button that will display the camera associated with the alarm point.

B. Display mouse-selectable icons representing each camera source, to select source to be displayed.

C. Allow cameras with preset positioning to be defined by displaying a different icon for each of the presets. Provide control with Next and Previous buttons to allow operator to cycle quickly through the preset positions.

2.11 EXAMINATION:

A. Examine roughing-in for LAN and control cable conduit systems to PCs, controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.
B. Proceed with installation only after unsatisfactory conditions have been corrected.

2.12 PREPARATION:

A. Comply with recommendations in SIA CP-01.
B. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.
1. Record setup data for control station and workstations.
2. For each Location, record setup of controller features and access requirements.
3. Propose start and stop times for schedules and holidays and match up access levels for doors.
4. Set up groups, facility codes, linking, and list inputs and outputs for each controller.
5. Assign action message names and compose messages.
6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
7. Prepare and install alarm graphic maps.
8. Develop user-defined fields.
9. Develop screen layout formats.
10. Propose setups for guard tours.
11. Discuss badge layout options; design badges.
12. Complete system diagnostics and operation verification.
13. Prepare a specific plan for system testing, startup, and demonstration.
14. Develop acceptance test concept and, on approval, develop specifics of the test.

15. Develop cable and asset-management system details; input data from construction documents. Include system schematics and CAD Technical drawings in electronic format.
16. In meetings with Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

2.13 **MOUNTING HEIGHTS**

A. Mounting heights must conform to ADA requirements.
B. Mounting heights must be from floor to center of device, unless otherwise noted. Verify exact locations and mounting heights with the Engineer/Owner before installation.
C. Unless otherwise noted, wall mounted devices requiring operational access must be mounted 48 inches above finished floor (interior) or grade (exterior) to highest operable portion of device.

2.14 **CABLING**:

A. Comply with NECA 1, "Good Workmanship in Electrical Construction."
B. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.
C. Install LAN cables using techniques, practices, and methods that are consistent with Category 6 rating of components and fiber-optic rating of components, and that ensure Category 6 and fiber-optic performance of completed and linked signal paths, end to end.
D. Boxes and enclosures containing security-system components or cabling, and which are easily accessible to employees or to the public, must be provided with a lock. Boxes above ceiling level in occupied areas of the building must not be considered accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public must be covered with a suitable cover plate and secured with tamperproof screws.
E. If required, install end-of-line resistors at the field device location and not at the controller or panel location.

2.15 **CABLE APPLICATION:**

A. Comply with TIA 569-B, "Commercial Building Standard for Telecommunications Pathways and Spaces."
B. Cable application requirements are minimum requirements and must be exceeded if recommended or required by manufacturer of system hardware.
C. RS-485 Cabling: Install at a maximum distance of 4,000 ft. (1220 m).
D. Card Readers and Keypads:
1. Install number of conductor pairs recommended by manufacturer for the functions specified.Unless manufacturer recommends larger conductors, install No. 22 AWG wire if maximum distance from controller to the reader is 250 ft. (75 m), and install No. 20 AWG wire if maximum distance is 500 ft. (150 m).
2. Install minimum No. 18 AWG shielded cable to readers and keypads that draw 50 mA or more.
E. Install minimum No. 16 AWG cable from controller to electrically powered locks. Do not exceed 500 ft.
F. Install minimum No. 18 AWG ac power wire from transformer to controller, with a maximum distance of 25 ft.

2.16 **GROUNDING:**

A. Comply with IEEE 1100, "Recommended Practice for Power and Grounding Electronic Equipment."
B. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.
C. Bond shields and drain conductors to ground at only one point in each circuit.
D. Signal Ground:
1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.
2. Bus: Mount on wall of main equipment room with standoff insulators.

3. Backbone Cable: Extend from signal ground bus to signal ground terminal in each equipment room and wiring closet.

2.17 **INSTALLATION:**

A. Install card readers, keypads, control panels, push buttons, and any related equipment, components necessary to complete the systems installation.

2.18 **IDENTIFICATION:**

A. Develop cable administration drawings for system identification, testing, and management. Use unique, alphanumeric designation for each cable, and label cable and jacks, connectors, and terminals to which it connects with the same designation. Use logical and systematic designations for facility's architectural arrangement.

B. Label each terminal strip and screw terminal in each cabinet, rack, or panel.

1. All wiring conductors connected to terminal strips must be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device must be identified with the name and number of the particular device as shown.
2. Each wire connected to building-mounted devices is not required to be numbered at the device if the color of the wire is consistent with the associated wire connected and numbered within the panel or cabinet.

C. At completion, cable and asset management software must reflect as-built conditions.

D. A copy of wire termination designations must be placed inside the cabinet door cover with real world logical locations and associated designation ID's.

E. Provide serial numbers, MAC addresses, frequency channels, time channels and duty cycles where applicable for all installed devices.

2.19 **SYSTEM SOFTWARE AND HARDWARE:**

A. Develop, install, and test software and hardware, and perform database tests for the complete and proper operation of systems involved. Assign software license to Owner.

2.20 **FIELD QUALITY CONTROL:**

A. Perform tests and inspections.

1. Manufacturer's Field Service: Engage a factory-authorized service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

B. Tests and Inspections:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 6 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA 568-B.1, "Commercial Building Telecommunications Cabling Standards - Part 1: General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA 568-B.1.
2. Test each circuit and component of each system. Tests must include, but are not limited to, measurements of power-supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup must be operated on battery power for a period of not less than 10% of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
   a. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

C. Devices and circuits will be considered defective if they do not pass tests and inspections.

D. Prepare test and inspection reports.

2.21 **STARTUP SERVICE:**

A. Engage a factory-authorized service representative to supervise and assist with startup service.

1. Complete installation and startup checks according to approved procedures that were developed in "Preparation" Article and with manufacturer's written instructions.

2. Enroll and prepare badges and access cards for Owner's operators, management, and security personnel.

2.22 **FINAL PUNCHLIST:**

A. Prior to Final Punch list, certify that systems and equipment are complete, operational, and are in compliance with the Contract Documents. Additionally, complete the following:
   1. Submit complete Operation and Maintenance Data.
   2. Submit complete Record Drawings.
   3. Perform all required training of Owner's personnel.
   4. Turn over all spares and extra materials to the Owner, along with a complete inventory of spares and extra materials being turned over.

B. During the Final Punch list, provide personnel with access keys, credential, handheld radios, and necessary expertise to operate each system and piece of equipment to demonstrate operational compliance with the Contract Documents.

C. Any deficiencies noted on the Final Punch list must be expeditiously corrected and certified in writing.

2.23 **ACCPETANCE:**

A. Perform all tests required by Owner in addition to tests specified herein.

B. Provide a minimum of 2 technicians on-site for each test and demonstration. Technicians shall be ready with all necessary tools, test equipment, and supplies necessary to troubleshoot and correct system faults after testing is completed. System must remain unaltered during testing at each site. Initial integration and testing is a one-time fee, as identified in Appendix D, Cost Proposal Form. All required testing, integration, and system updates shall be considered part of the City's ongoing maintenance program, as provided by the successful Contractor(s), at no additional cost to the City.

C. Upon receipt of the Contractor's documentation of system testing, the Owner and Engineer will review/observe the installation and randomly request test and demonstration of the system installed. Once all tests have been passed in accordance with sections in Division 28 and the Owner is satisfied that all work is in accordance with the Contract Documents, The Owner will notify the Contractor in writing that the work has been accepted.

D. Engage a factory-authorized service representative to train owner's maintenance personnel to adjust, operate, and maintain security access system.

E. Develop separate training modules for the following:
   1. Computer system administration personnel to manage and repair the LAN and databases and to update and maintain software.
   2. Operators who prepare and input credentials to man the control station and workstations and to enroll personnel.
   3. Security personnel.
   4. Hardware maintenance personnel.
   5. Corporate management.

F. Provide video and audio recording of all training modules. Index and edit recording to inject relevant graphics, examples, and additional commentary to produce a useful training video. Indexing should be by topic and subsystem presented allowing viewer to select portion of training video they wish to review. Provide four copies of video in DVD format that can be played on consumer grade DVD players and PCs. Place no restrictions on Owner's rights to reproduce DVD for Owner's use.

Balance of Page Intentionally Left Blank

C. Special Conditions.

1. Term. Any resulting contract shall remain in effect for five (5) years from the effective date contingent upon funding is available as appropriated on an annual basis. Prior to, or upon completion, of that initial term, the City shall have the option to renew this contract for an additional five (5) one (1) year(s) periods, on a year-to-year basis. Continuation of the contract beyond the initial period, and any option subsequently exercised, is a City prerogative, and not a right of the vendor. This prerogative may be exercised only when such continuation is clearly in the best interest of the City.

Balance of Page Intentionally Left Blank

APPENDIX E

MIAMIBEACH

Insurance Requirements

RFQ 2020-009-JC
Citywide Security Access Software System

PROCUREMENT DEPARTMENT
1755 Meridian Avenue, 3rd Floor
Miami Beach, Florida 33139

MIAMIBEACH

INSURANCE REQUIREMENTS

This document sets forth the minimum levels of insurance that the contractor is required to maintain throughout the term of the contract and any renewal periods.

XXX 1. Workers' Compensation and Employer's Liability per the Statutory limits of the state of Florida.

XXX 2. Comprehensive General Liability (occurrence form), limits of liability $ 1,000,000.00 per occurrence for bodily injury property damage to include Premises/ Operations; Products, Completed Operations and Contractual Liability. **Contractual Liability** and Contractual Indemnity (Hold harmless endorsement exactly as written in "insurance requirements" of specifications).

XXX 3. Automobile Liability - $1,000,000 each occurrence - owned/non-owned/hired automobiles included.

____ 4. Excess Liability - $_____.00 per occurrence to follow the primary coverages.

XXX 5. The City must be named as and additional insured on the liability policies; and it **must** be stated on the certificate.

____ 6. Other Insurance as indicated:

___ Builders Risk completed value	$_____.00
___ Liquor Liability	$_____.00
___ Fire Legal Liability	$_____.00
___ Protection and Indemnity	$_____.00
___ Employee Dishonesty Bond	$_____.00
___ Other	$_____.00

XXX 7. Thirty (30) days written cancellation notice required.

XXX 8. Best's guide rating B+:VI or better, latest edition.

XXX 9. The certificate must state the proposal number and title

The City of Miami Beach is self-insured. Any and all claim payments made from self-insurance are subject to the limits and provisions of Florida Statute 768.28, the Florida Constitution, and any other applicable Statutes.

APPENDIX F

MIAMIBEACH

System Requirements Matrix

RFQ 2020-009-JC
Citywide Security Access Software System

PROCUREMENT DEPARTMENT
1755 Meridian Avenue, 3rd Floor
Miami Beach, Florida 33139

APPENDIX F SECURITY ACCESS CONTROLS SYSTEM REQUIREMENTS		
SPECIFICATIONS REQUIREMENTS	**Does Proposed System/Equipment Meet Requirement?**	
	Yes	**No**
Multiuser and multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations		
Graphical user interface to show pull-down menus and a menu-tree format that complies with interface guidelines of Microsoft Windows.		
System license for the entire system including capability for future additions that are within the indicated system size limits specified.		
Open-architecture system that allows importing and exporting of data and interfacing with other systems that are compatible with Microsoft		
Password-protected operator login and access.		
Open-database-connectivity compliant.		
PACS FIELD HARDWARE	**Yes**	**No**
The PACS shall be equipped with the access control field hardware required to receive alarms and administer all access granted or denied decisions.		
Intelligent Controllers a.Native network support and is scalable to 64 doors/openings. b.OSDP Protocol secure channel security for reader connectivity. c.On-board Ethernet port to connect to server-based access control hosts. d.Performs access control, alarm management and scheduled operations. e.600,000 cardholder capacity f.Supports up to 1024 inputs and 1024 outputs.		
Intelligent Controller w/ Extended Applications a.Supports a variety of extended features including High Assurance Credential Authentication. b.OSDP Protocol secure channel security for reader connectivity and extended applications. c.Direct hardware support for 2 doors/openings and can scale to 64 doors/openings. d.Performs access control, alarm management and scheduled operations. e.On-board Ethernet port to connect to server-based access control hosts. f.2,000,000 cardholder capacity g.Supports up to 1024 inputs and 1024 outputs		

Edge-capable Intelligent Controllers a.Expandable up to 8 downstream serial input/output modules and expandable up to 17 doors/openings. b.OSDP Protocol secure channel security for reader connectivity. c.POE+ capable. d.240,000 cardholder capacity. e.Supports up to 130 inputs and 130 outputs.		
Input Controller Module a.Provides 16 general purpose input circuits. b.Inputs can be set for normally open or normally closed. c.Inputs can be declared supervised or non-supervised.		
Output Control Module a.Provides 16 general purpose outputs as Form C relay contacts. b.Individually configurable parameters that can be set for timing and for fail-safe versus fail secure modes.		
Single Reader Interface Panel. a.RS-485 connected and can be clustered or distributed depending on the installation requirements. b.OSDP Protocol secure channel security for reader connectivity. c.Provides all I/O needed for single door control.		
Dual Reader Interface Panel. a.Provides all I/O needed for controlling two doors with auxiliary point control and monitoring. b.RS-485 Connected. c.OSDP Protocol secure channel security for reader connectivity.		
Data Line Problems: For periods of loss of communication with the access server, or when data transmission is degraded and generating continuous checksum errors, the controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.		
OPERATION	**Yes**	**No**
Security access system shall use a single database for access-control and credential-creation functions.		
Security access system shall be capable of accessing Active Directory for credential-creation and functions.		
Access-control information, including time, date, valid codes, access levels, and similar data, shall be downloaded to controllers so each controller can make access-control decisions.		
In the event that communications with the central server is lost, controllers shall automatically buffer event transactions until communications are restored, at which time buffered events shall be uploaded to the access server.		

Each controller shall have its own database and history.		
System components shall be interconnected and shall provide automatic communication of status changes, commands, field-initiated interrupts, and other communications required for proper system operation.		
Communication shall not require operator initiation or response and shall return to normal after partial- or total-network interruption such as power loss or transient upset.		
System shall automatically communicate failures to the operator and shall identify the communications link that has experienced a partial or total failure.		
Central server shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central server shall control system networks to interconnect all system components, including workstations and field-installed controllers.		
Alarms shall be communicated at the central server within three second of the alarm occurring at a controller or at a device controlled by a local controller, and within 1 second if the alarm occurs at the central server.		
Alarm and status changes shall be displayed within 1 second after receipt of data by the central server.		
All graphics shall be displayed, including graphics-generated map displays, on the console monitor within five seconds of alarm receipt at the security console.		
Equipment and software shall comply with SIA CP-01.		
System shall initiate an alarm in response to opening, closing, shorting, or grounding of data transmission lines.		
Electrical characteristics of controllers shall match the signal and power requirements of door hardware.		
Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-controller communications methods by changing the polling frequency and the amount of time the system waits for a response.		
WORKSTATION SOFTWARE	**Yes**	**No**
User levels shall be individually customized by login credentials to allow or disallow operator access to program functions for each Location.		
Workstation event filtering shall allow user to define events and alarms that will be displayed at each workstation.		
CONTROLLER SOFTWARE	**Yes**	**No**
Controllers shall operate as autonomous, intelligent processing units.		

Controllers shall make decisions about access control, alarm monitoring, linking functions, and door-locking schedules for their operation, independent of other system components		
Controllers shall be part of a fully distributed (and routable) processing-control network.		
The portion of the database associated with a controller, and consisting of parameters, constraints, and the latest value or status of points connected to that controller, shall be maintained in the controller.		
The following functions shall be fully implemented and operational within each controller: a.Monitoring inputs. b.Controlling outputs. c.Automatically reporting alarms to the central server. d.Reporting of sensor and output status to the central server on request. e.Maintaining real time, automatically updated by the central server at least once a day. f.Communicating with the central server. g.Diagnosing. h.Downloading and uploading data to and from the central server.		
Linking and anti-pass back shall remain fully functional within the same Location even when the central server or workstations are off-line.		
Controllers at each Location shall be connected to a memory buffer with a capacity to store up to 10,000 events; there shall be no loss of transactions in system history files until the buffer overflows.		
Controllers shall transmit alarms, status changes, and other data to the central server when communications circuits are operable.		
If communications are not available, controllers shall function in a stand-alone mode; operational data, including the status and alarm data normally transmitted to the central server, shall be stored for later transmission to the central server.		
Storage capacity for the latest 1,024 events shall be provided at each controller.		
Controllers shall provide a response to card readers or keypad entries in less than 0.25 second, regardless of system size.		
Controllers that are reset, or powered up from a nonpowered state, shall automatically request a parameter download and reboot to their proper working state. This shall happen without any operator intervention.		
System shall monitor and report status of RS-485 communications loop of each Location.		
Communication status window shall display which controllers are currently communicating, a total count of missed polls in a user configurable time period, and which controller last missed a poll.		
Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM for each controller.		

Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month.		
The real-time clock shall be automatically synchronized with the central server at least once a day to ±10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.		
All data transmissions from PCs to a Location, and between controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.		
Software shall provide for setting downloads via dial-up connection to once per 24-hour period, with time selected by the operator.		
Software shall provide for setting delays of database downloads for dial-up connections. Delays change the download from immediately to a delay ranging from one to 999 min.		
OPERATOR INTERFACE	**Yes**	**No**
System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.		
Icon shall change automatically to show the live summary status of points in that group.		
Override group icon shall provide a method to manually control or set to time-zone points in the group.		
Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.		
To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.		
Each schedule shall be composed of a minimum of two dates with separate times for each date.		
The first time and date shall be assigned the override state that the point shall advance to when the time and date become current.		
The second time and date shall be assigned the state that the point shall return to when the time and date become current.		
REPORTS	**Yes**	**No**
Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm (such as door alarm, intrusion alarm, tamper alarm, etc.), the type of sensor, the location, the time, and the action taken.		

The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.		
Each report shall depict the date, time, event type, event description, and device; or I/O name, cardholder group assignment, and cardholder name or code number.		
Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.		
Total number of lines of the report shall be given at the end of the report.		
Reports shall have the following four options: a.View on screen. b.Print. Include automatic print spooling and "Print To" options if more than one printer is connected to the system. c."Save to File" with full path statement. d.System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that are abnormal, out of schedule, manually overridden, not reporting, or in alarm.		
The reports of system database shall allow options so that every data field may be printed.		
The reports of system database shall be constructed so that the actual position of the printed data shall closely match the position of the data on the data-entry windows		
Database management functions shall allow operators to add, delete, and modify access data as needed.		
The enrollment station shall not have alarm response or acknowledgment functions.		
Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.		
The program shall provide means to disable the enrollment station when it is unattended, to prevent unauthorized use.		
The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations.		
The data field names shall be customized during setup to suit user and site needs.		
Personnel identity-verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files		

System shall have the ability to run searches and reports using any combination of these fields. Each user-defined field shall be configurable, using any combination of the following features: a.MASK: Determines a specific format with which data must comply. b.REQUIRED: Operator is required to enter data into field before saving. c.UNIQUE: Data entered must be unique. d.DEACTIVATE DATE: Data entered will be evaluated as an additional deactivate date for all cards assigned to this cardholder. e.NAME ID: Data entered will be considered a unique ID for the cardholder.		
The results of each test shall be stored for future display or printout. The report shall document the operational status of system components.		
Reports shall be stored by type, date, and time.		
Report printing shall be the lowest-priority activity. Report-generation mode shall be operator selectable but set up initially as periodic, automatic, or on request.		
SYSTEM DATABASE	**Yes**	**No**
File management shall include database backup and restoration system, allowing selection of storage media, including CDR, DVD, or USB drive, and designated network resources.		
Operations shall be both manual and automatic modes.		
Backup program shall provide manual operation from any PC on the LAN and shall operate while system remains operational		
Access authorization shall be by card, by a manually entered code (PIN), or by a combination of both (card plus PIN).		
Access authorization shall verify the facility code first, the card or card-and-PIN validation second, and the access level (time of day, day of week, date), and number of uses last.		
Use data-entry windows to view, edit, and issue access levels. Access-authorization entry-management system shall maintain and coordinate all access levels to prevent duplication or the incorrect creation of levels.		
Software shall allow the grouping of locations to allow cardholder data to be shared by all locations in the group.		
Photo ID badging and photo verification shall use the same database as the security access and may query data from cardholder, group, and other personal information to build a custom ID badge.		
Automatic or manual image recall and manual access based on photo verification shall also be a means of access verification and entry.		
System shall allow sorting of cardholders together by group or other characteristic for a fast and efficient method of reporting on, and enabling or disabling, cards or codes.		

System shall accommodate up to 2,048 facility codes per Location, with the option of allowing facility codes to work at all doors or only at particular doors.		
System shall have a minimum of 999 predefined operator comments with up to 30 characters per comment.		
System software shall have the capacity to assign one of 32,000 group names to an access authorization.		
System shall have the capacity for 2,048 schedules for each Location.		
System shall have the capacity for 255 annual holidays.		
System shall allow for the creation of up to 32,000 access levels		
System shall allow for access to be restricted to any area by reader and by time.		
System shall be able to create multiple door and time-zone combinations under the same access level so that an Identifier may be valid during different time periods at different readers even if the readers are on the same controller.		
System shall provide a minimum of 99 user-defined fields, each with up to 50 characters, for specific information about each credential holder.		
System shall accommodate a title for each field; field length shall be 20 characters.		
System shall have the ability to print cardholders based on and organized by the user-defined fields.		
PROJECT CONDITIONS	**Yes**	**No**
System shall be capable of withstanding the following environmental conditions without mechanical or electrical damage or degradation of operating capability:		
Control Station: Rated for continuous operation in ambient conditions of 60 to 85°F (16 to 30°C) and a relative humidity of 20 to 80%, noncondensing.		
Indoor, Uncontrolled Environment: Type 3R enclosures. System components installed in non-air-conditioned, non-temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of [0 to 122°F (-18 to +50°C) dry bulb and 20 to 90% relative humidity, noncondensing.		
Outdoor Environment: NEMA 250, NEMA 250, Type 4 enclosures. System components installed in locations exposed to weather shall be rated for continuous operation in ambient conditions of -30 to +122°F (-34 to +50°C) and 20 to 90% relative humidity, condensing. Rate for continuous operation where exposed to rain as specified in NEMA 250, winds up to 85 mph (137 km/h) [and snow cover up to 24 inches (610 mm) thick].		
CARD READER PRODUCT	**Yes**	**No**
Card reader shall respond to passage requests by generating a signal that is sent to the controller.		

Response time shall be 800 ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.		
TAMPER PROTECTION	**Yes**	**No**
Tamper switches on enclosures, control units, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled.		
Control-station control-unit alarm display shall identify tamper alarms and indicate locations.		