सत्यमेव जयते

Embassy of India
Muscat, Oman

www.indemb-oman.gov.in

TENDER FOR UP-GRADATION OF EXISTING ACCESS CONTROL SYSTEM INSTALLED IN EMBASSY OF INDIA, MUSCAT, SULTANATE OF OMAN

Tender No. : MUS/815/01/2021

Date: 17th July, 2024

Last date for submission of bids: 07th August, 2024

Embassy of India, Muscat, Oman
Diplomatic Area, Jamiat, Al Dowal Al-Arabia Street. PO Box No.
1727, Postal Code 112, Al Khuwair, Sultanate of Oman

सत्यमेव जयते

EMBASSY OF INDIA
MUSCAT
***

No. MUS/815/01/2021 **Date: 17.07.2024**

Notice Inviting Tender

Subject: Up-gradation of existing Access Control System installed in the Chancery of Embassy of India, Muscat.

Embassy of India, Muscat invites tenders under two bid system (Technical and Financial), from registered and authorized companies for 'Up-gradation of existing Access Control System installed in the Chancery of Embassy of India, Muscat'.

IMPORTANT DATES

S.No.	**Events**	**Date**
1.	Tender Publish Date	17th July 2024
2.	Site visit	On any working day before bid closing date (0900 – 1700hrs on working days from Sunday to Thursday)
3.	Bid Submission start date	17th July 2024
4.	Bid Submission end date	07th August 2024 (till 1700 hrs)
5.	Opening of Technical Bids	08th August 2024(at 1500 hrs)
6.	Opening of Financial Bids (of only those who qualify in the minimum eligibility criteria)	Date to be intimated later

2. The tender document can be downloaded from the websites: http://www.eprocure.gov.in and http://www.indemb-oman.gov.in from 17th July, 2024 onwards i.e. ***from July 17, 2024 to August 07, 2024*. No tender fee will be charged for the tender documents** in case a company has downloaded the tender document from the official website of the Embassy of India, Muscat, i.e. www.indemb-oman.gov.in. Please note that any corrigendum/addendum in the above tender document, if required, will be published on the website of the Embassy of India, Muscat, as given above.

3. The interested firms/companies should submit the bids in two separate sealed covers, superscribed as “Technical Bid” and “Financial Bid”. Both sealed covers should be put in a single envelope superscribed as “Tender No. MUS/815/01/2021 for “**Up-gradation of existing Access Control System installed in the Chancery of Embassy of India, Muscat**” and addressed to “Head of Chancery, Embassy of India, Muscat Diplomatic Area, Al-Khuwair, Muscat, Oman”. The envelope should then be dropped at the Reception of the Embassy of India, Muscat at the address given above. Please note that tender document will not be accepted after the expiry of stipulated date and time under any circumstances.

4. The Earnest Money Deposit (EMD) of OMR 200/- (Omani Rial Two Hundred only) in the form of Account Payee Demand Draft/Pay Order drawn in favour of **“Embassy of India, Muscat”** is required to be submitted along with tender bids. Bids shall not be considered in case the EMD is not submitted and would be rejected summarily.

5. The bidders have an option to submit, in lieu of EMD of RO 200/-, a judicially valid Undertaking to the effect that if they withdraw or modify their bids during the period of validity, or if they are awarded the contact and they fail to sign the contract, or to submit a performance security before the stipulated deadline, they will be suspended for a specified time period from being eligible to submit bids for contracts with the Embassy of India, Muscat.

6. The Technical Bids will be opened on **08th August 2024** by a Committee authorized by the Competent Authority of the Embassy. The financial bids of only those bidders, whose Technical Bids are found responsive, shall be opened by the Committee authorized for the purpose.

7. The Competent Authority reserves the right to reject any or all the bids, or cancel the tender, without assigning any reason and the decision of the competent authority of the Mission/Ministry shall be final and binding.

(Pardeep Kumar)
First Secretary (HOC)
Embassy of India
Muscat

Tel No. +968-24684566

LETTER OF BID

Dated: 17th July, 2024

To,
Shri Pardeep Kumar
First Secretary (HOC)
Embassy of India,
Diplomatic Area, Al-Khuwair
Muscat, Sultanate of Oman

Ref: Invitation for Bid No. MUS/815/01/2021 dated 17th July 2024.

We, the undersigned, declare that:

We have examined and have no reservations to the Bidding Documents, including Addendum issued in accordance with Instructions to Bidders,

2. We offer to execute in conformity with the Bidding Documents for **Up-gradation of existing Access Control System installed in the Chancery of Embassy of India, Muscat.**

3. Our bid shall be valid for a period of 180 days from the date fixed for the bid submission deadline in accordance with the Bidding Documents and shall remain binding upon us and maybe accepted at any time before the expiry of the period.

4. If our bid is accepted, we commit to submit a Performance Security Deposit (if any) in accordance with the Bidding Documents.

5. We also declare that the Government of India, Govt of Sultanate of Oman or any other Government body has not declared us ineligible or blacklisted us on charges of engaging in corrupt, fraudulent, collusive or coercive practices or any failure/lapses of serious nature.

6. We also accept all the terms and conditions of this bidding document and undertake to abide by them, including the condition that you are not bound to accept highest ranked bid/lowest bid or any other bid that you may receive.

Yours sincerely,

Authorized Signatory

(Authorised person shall attach a copy of Authorization for signing on behalf of Bidding company)
Full Name and Designation
(To be printed on Bidder's letterhead)

SECTION I: CRITERIA FOR SELECTION

1. The company must have experience of commissioning similar kind of work in reputed organizations and shall have minimum eligibility criteria for selection of bidders at technical bid stage of the bidding process:-

2. **Legally Valid Entity:** The Bidder/Bidding company shall necessarily be a legally valid entity either in the form of a Limited Company or a Private Limited Company registered under the relevant Act or a firm having trade license granted by competent authority of Government of Sultanate of Oman to do business in Muscat. The proof for supporting the legal validity of the Bidder/Bidding company shall be attached with the bid.

3. **Registration:** The Bidder/Bidding company must have CR and VAT registration with the concerned authority in Oman. The proof in support of the same shall be attached with the bid documents.

4. **Experience:** The Bidder may have experience in supplying and installing security related equipment for Embassies /High Commissions /Government Ministries /Departments /Public Sector Companies /reputed corporate organization /multinational companies.

5. **Company profile/information regarding key personnel:** The bidding company shall also include in its bid, as per proforma at Annexure-5 (Technical bid proforma) of this document, details about the company and about its key personnel.

6. The persons deployed by the company to perform the work should have requisite experience and skills for carrying out the assigned up-gradation of access control system. The contractor must employ adult and skilled labour only.

7. Rates quoted shall be firm and fixed. No escalation of whatsoever nature shall be payable.

8. The competent authority reserves the right to withdraw/relax any of the terms and conditions mentioned in the tender document.

9. For finalization of work, the company whose rates are the lowest in comparison to other companies will be considered as the lowest bidder.

10. This Mission reserves the right to cancel the work order in any eventuality, without any notice and without explaining any reasons to the Company. The Company shall not have claim for any compensation in such event of cancellation of the work order.

11. The interested companies should submit the bids in two separate sealed covers, superscribed as ‘Technical Bid’ containing duly filled in **Annexure-5** and ‘Financial Bid’ containing duly filled in **Annexure-2**. Both sealed covers should be put in a single envelope

super scribed as “Tender No. MUS/815/01/2021 for “**Up-gradation of existing Access Control System installed in the Chancery of Embassy of India, Muscat**” and addressed to ‘Head of Chancery, Embassy of India, Muscat’. The bids should be submitted to the Head of Chancery, Embassy of India, Jami’at Al dowal Al -Arabiya Street, Diplomatic Area, Al Khuwair, P.O. Box 1727, PC:112, Muscat. Please note that **no** tender documents will be accepted after the expiry of stipulated date and time for the purpose i.e. **August 07, 2024,** under any circumstances.

12. The Technical Bids will be opened on **August 08, 2024** at **1500 hrs** by a Committee duly constituted by the Competent Authority of the Embassy of India, Muscat. The Financial Bids of only those bidders, whose Technical Bids are found responsive, shall be opened by the Committee authorized for the purpose.

13. **EARNEST MONEY DEPOSIT(EMD):** The Earnest Money Deposit of RO 200/- (Omani Rial Two Hundred only) in the form of account Payee Demand Draft/Pay order issued by any reputed Bank drawn in favour of “Embassy of India, Muscat” has to be submitted along with the bid. The validity of the Demand Draft/Pay Order must be up to 6(six) months from the last date for submission of bids.

13.1 The bids without Earnest Money Deposit or the Undertaking will be summarily rejected.

13.2 No claim shall lie against the Mission in respect of erosion in the value or interest on the amount of earnest money deposit or security deposit i.e. no interest will be payable on EMD.

****** End of Section ******

SECTION II : SCOPE OF WORK

DETAILED SPECIFICATIONS OF VARIOUS COMPONENTS REQUIRED FOR ACCESS CONTROL SYSTEM

1. Face Recognition Device

S.no	Feature	Specifications
1.	Types of Face Cameras	Device should have visual face recognition camera able to detect human face. Must include lighting (IR and Optical) in order to be able to recognize faces in all environments (from dark to light).
2.	Face algorithm False Accept/Reject Rates	Should be Face Recognition Technology and Evaluation (FRTE) [1:N Identification] compliant issued by National Institute of Standards and Technology (NIST) of USA or better.
3.	Face Reading Timing	Should be less than 1 second/face.
4.	Face Recognition with Mask	Facial recognition shall work with COVID-19 type of face masks.
5.	Face Enrollment	Physical presence should be must for face enrollment. The system should have deactivation facility for registration without physical presence. The system shall be able to distinguish between human face and other face imprints such as paper, OHP film, glue, rubber, clay and silicon etc.
6.	Live Face Detection – Anti spoofing	Should have anti spoofing feature for live face detection/rejection of false faces.
7.	Display Type	Minimum 5" screen or better.
8.	Housing Material / Enclosure	Sealed proof case with IP65 rating or better as per OEM.
9.	Certification / Safety Standard	Required certifications of product - CE, FCC, RoHS and WEEE.
10.	Firmware Upgrades	Should have upgrade facility for offline-mode and deactivation of remote upgradation of software.
11.	Configuration/ Web Server	Device should have in-built GUI interface for configuration or changes at installation site with facility of deactivating any remote configuration / management.
12.	Security features	Data exchanges between equipment and server shall be encrypted as per AES256, TLS1.2 or equivalent or better protocol.
13.	Tamper	Tampering detection alert should be there at server end.
14.	Microphone / Wi-Fi/ Bluetooth / Mobile Access / PIN Code option / QR Code for Visitors / RF Card options	If present, should have facility of deactivation.

15.	Network Interface	TCP/IP (Ethernet RJ-45 – POE Interface) with IPv4.0 (Optional: IPv6.0) compatible, Wiegand interface, RS485 / RS232 or higher
16.	Authentication Options / Biometrics	Programmable for defining authentication options with facility of deactivation.
17.	Mounting	Mounting arrangements should be as per location and requirements.
18.	DI/DO Ports (For relay of signals)	Min 1 or more internal output relay (NC/NO) for door control and minimum 2 or more programmable I/O for connecting external devices such as Fire Alarm, Detection, NVR etc.

2. SERVER

S.No.	Feature	Specifications
•	Type of Server/Form Factor	Tower Type Chassis
•	Processor	Core i9 Processor 13th Gen, 3.0GHz or better
•	Memory	32 GB DDR4 RAM or better
•	Hard Drives	450 GB SSD or better **AND** 2 TB SATA or better
•	Graphic Card	Min 4GB or better Graphics Card with HDMI / Mini DP Ports
•	Network Adapter Card (NIC)	Minimum 2 or More 100/1000 Mbps NIC Cards
•	Keyboard	USB Keyboard.
•	Mouse	Optical Mouse with scroll.
•	Operating System	Licensed MS Windows 10 or better / Linux - compatible with access control software.
•	Anti Virus Software	Anti-virus software compatible with Windows/Linux with offline updates provision.
•	Display Type	27 inches or more screen with 2x HDMI / DP Ports.

3. POE SWITCHES

S.No.	Feature	Specifications		
4.	PoE Port	8*10/100/1000 port	16*10/100/1000 port	24*10/100/1000 port
5.	Switch Type	Managed Switch	Managed Switch	Managed Switch
6.	Switch Capacity	5 Gbps or better	7 Gbps or better	8 Gbps or better
7.	Transmission Distance	100-150m		
8.	Protocol Standards	IEEE802.3, IEEE02.3u, 802.3x, IEEE802.3 af / IEEE802.3 at		
9.	PoE Power	Min 30 W or more power per port		
10.	Network Medium	10/100/1000 Mbps 5 class and above non shielded twisted pair		
11.	Port Configuration	Power priority mechanism, fast and forward, MAC		

		IEEE802.3X full duplex and mode and back pressure for half duplex mode
12.	Indicators	Each port occupied 1 Link/Act 100 Mbps POE status indicator, whole power indicator.

4. PASSIVE ITEMS

S.No.	Feature	Specifications
a.	Power Cable	3 Core 1.5 Sq. mm PVC copper multi-core circular sheathed cable with rigid conductor.
b.	CAT 6 UTP Cable	4 pair cable with speed 100 mbps or better.
c.	Patch Cords	Cat 6 patch cord
d.	Wall Mount Rack	9U outdoor / indoor wall mount rack for switches with power distribution units (PDU) and accessories, minimum 60 Kg load bearing capacity

5. LOCKS

S.No.	Feature	Specifications
•	Types of Locks	Single Door Lock Double Door Lock Drop Bolt Lock
•	Mechanism	Fail secure locking facility Normally Closed (NC)
•	Integration	Integration with Access Control System (ACS)
•	Installation	Should be easily installable on any type of door i.e. wooden, aluminum or steel door.
•	Cycles Tested	500,000 cycles or more.
•	Mechanical Key	Mechanical override cylinder – having one physical master key to operate in case of emergency.
•	Tensile Strength Resistance	Upto 1000 Kgs.
•	Bluetooth/Wifi feature etc, if available	Should have facility of deactivating all such features.

6. OPERATING SOFTWARE

S. No.	Specifications
1.	ACS software should be browser based with supporting databases.
2.	ACS software should be able to manage biometric, card reader and controllers with same software. User enrollment should be done only once for biometric and controller enrollment.

3.	ACS software should have functionality to import existing user/terminal details from excel sheet or existing database. The API should also be available to expose to 3rd party system to Pull/Push logs.
4.	ACS software should have support to migrate biometric & images from existing system and seamless migration to future biometric systems.
5.	ACS software should be able to PULL biometric templates from device to central database.
6.	ACS software should be able to show user details, enrollment status of biometrics , duress finger, biometric modality etc.
7.	ACS software should be able to show user wise logs.
8.	ACS software should be able to show given user present in list of terminals.
9.	ACS software should be able to ACS add, delete or edit user from the interface.
10.	ACS software should be able to filter enrolled and non-enrolled users.
11.	ACS software should be able to use any IP based device or USB biometric device for enrolment
12.	ACS software should be able to capture photograph, demographic details, biometric (Fingerprint (Upto 10 Fingers and mark duress finger to one of them) / Face / IRIS etc) modalities
13.	ACS software should be able to do card encoding & reading
14.	ACS software should be able to assign user wise policy - a user may have different access policies for different readers. It should be configurable. For example user A may have finger + card on one terminal and finger only on another terminal.
15.	ACS software should be able to assign different user policy on same terminal. For example: user A may have finger only policy and user B may have finger+ card policy on same terminal.
16.	ACS Software should be able to assign a specific access schedule to user.
17.	ACS Software should have an option to delete biometric and re-enroll them whenever needed.
18.	ACS software should be able to push user/group of users in terminal/group of terminals.
19.	ACS software should be able to show the terminal list with online and offline status.
20.	ACS software should be able show count of online and offline Terminals.
21.	ACS software should be able to show/extract terminal wise logs.
22.	ACS software should be able to show/extract terminal wise user list.
23.	ACS software should be able to add/edit/delete terminal details.
24.	ACS Software should be able to do terminal wise wiegand settings.
25.	ACS software should be able to set global policies for all the terminal and should also

	have an option to set the local policies.
26.	ACS software should be able to add/delete user and terminal group.
27.	ACS software should be able to set group wise user/terminal policy.
28.	ACS software should be able to fetch real time logs directly from reader & controller.
29.	ACS software should be able to display user details along with photograph while real time identification.
30.	ACS software should never delete logs from reader; it should overwrite in FIFO mode when it reached the reader's maximum limit.
31.	ACS software should be fingerprint stored in the database and should be encrypted with 256 bit AES key. There should be an option to inject customer keys.
32.	ACS software should be able to integrate with existing and upcoming software
33.	ACS software should have facility for integration with CCTV camera at server end. Vendor to provide Application Programming Interface (API) and Software Development Kit (SDK) for integration purpose.

7. OTHER IMPORTANT POINTS

S.No.	Point
1.	Should always be used in ‘Offline’ mode.
2.	Should have facility of deactivating features like finger based access, cards based access, mobile based access, remote access for entry, bluetooth, WiFi, remote firmware upgrade, remote maintenance, remote server configuration, keypad, remote user enrolment etc. Bidder (once the tender is awarded to L-1) must submit an undertaking that after the system is operational, all these features would be deactivated.
3.	System should be connected to an UPS for continuous power supply including during power failure.
4.	The facility of auto deletion of record/record creation for a particular time frame/pop-up message when record reaching its expiry or after specified time limit is over should also be incorporated in operating software with option of fixing default time.
5.	Intellectual Property Rights (IPR) of brand(s) (back end and front end manufacturing) should not be with a company from a country which share land border with India.
6.	**Warranty**: 5 years OEM warranty or better
7.	**Integration**: Should have capability for integration with other security equipment such as fire alarm/panel etc.

8. BILL OF QUANTITY (BOQ)

The bill of quantities is as follows:

S.No.	Item	Quantity
1	Access Control Software	1
2	Main Door Controller 4 readers with network connectivity	1
3	Direct Controller 4 Readers	2
4	Biometric Face Recognition Device + Card Reader (Supports HID prox)	9
5	**Lock** : 600Lbs,12VDC/24VDC SURFACE MOUNT MAGNETIC LOCK with Z / L Bracket (as per required specifications)	8
6	DOOR CONTACT SURFACE	8
7	Touch less exit switch button	8
8	Conduit and cable for the above system (LOT)	01
9	Civil Work for the above (LOT)	01
10	Server (as per required specifications)	01
11	POE switch	Upto 4 ports will be provided by the Embassy. Additional ports, if required, will be provided by the vendor
12	Termination, Testing, Commissioning of the Hardware and Software including training at local office for the above system	01
13	Printing and supply of photo identity (RFID) cards with photo and other details provided by the Embassy	150

SECTION III : OTHER GENERAL INSTRUCTIONS

SYSTEM USER REQUIREMENTS

A. **System Overview:**

1. The contractor shall provide and install a new integrated security system. The new system shall be able to provide Access Control, Identity Management, Alarm Management, and other functionality in a single fully integrated Security Management System
2. The Security Management System shall have a simple, consistent and easy-to-use graphical user interface.
3. The manufacturer of the proposed system shall have produced access control products for at least 20 years.
4. The manufacturer shall be ISO 140001 certified indicating their commitment to conserve energy and reduce waste.
5. The Security Management System shall operate using a Microsoft SQL Server database and shall support Microsft SQLServer 2012 and SQLServer 2014
6. The System shall support virtualization using VMWare
7. The manufacturer of the proposed system shall require resellers to pass a formal training program prior to being certified as authorized to sell and install the system. Such certification shall require annual re-qualification. The system integrator proposing the system shall be in possession of such a certification.
8. The Security Management System client and server software shall be used in conjunction with intelligent controllers to provide a distributed access control and alarms monitoring system. In the event of a communications failure between the host server and the field controllers, the controllers shall continue to make local access control decisions and save all transactions in memory until communications are restored. At that time the controller shall upload all stored transactions to the server.
9. The Security Management System shall seamlessly integrate the functions of access control, alarms monitoring and response, video management, badge design/creation, identity management and visitor management. Licenses for all of these items (except for licenses for individual cameras) shall be included as part of the base price of the proposal, and not as extra-cost options.
10. All Security Management System user interface components shall run in an integrated application environment as part of a single application executable. Systems which provide their user interface through multiple separate applications programs shall not be acceptable, except as specifically indicated below.

B. Required Access Control Hardware Features

1. The Security Management System will provide the option of using either conventional modular door controllers which enable between 2 and 16 doors to

be housed within one steel enclosure or alternatively using Edge Network Controllers supporting PoE+.

2. The Security Management System intelligent database controller shall support a minimum of 20,000 cardholders with expansion capabilities of up to 1,000,000 cardholders.
3. The Security Management System intelligent database controller shall support a minimum of 12,000 offline transactions. The option to provide for at least 65,000 transaction storage at the panel must be available.
4. The Security Management System hardware shall be comprised of modular components that connect over standard interfaces to one another. There shall be database storage and processing module (DBU), and once data has been downloaded to the DBU it shall locally make access control decisions. Access granted or denied decisions shall be made in under 0.5 seconds.
5. The DBU shall store firmware in non-volatile flash memory to allow for convenient updates through a firmware update application. The DBU shall store the cardholder and configuration database information in battery-backed memory so that loss of primary power will not cause the loss of the database.
6. The Security Management System hardware shall be capable of expansion via 2-, 4-, and 8- door controllers (DC). Door controllers shall support one or more input/output module expansion cards that require no additional addressing and provide 8 monitored input points or 8 auxiliary output points.
7. The DBU shall support configurations that include: 16 card readers, 96 monitored input points, or 96 auxiliary output points.
8. There shall be an intelligent controller option to provide control of 8 readers/doors from a single circuit board (communications, memory, CPU, and reader/door functions integrated) with an available 8-reader/door add-on to provide a 16-door controller from two circuit boards. The 8-door controller shall provide an integrated on-board RS-232 interface, and shall have provisions for modular expandable memory.
9. System must support the installation of card readers at any distance up to 3000 feet from the reader interface board. Systems that do not support this requirement, or that require additional, separately mounted components to achieve the requirement shall not be acceptable. This requirement does not apply to biometric reader devices or Wiegand readers.
10. Each supplied card reader shall be continuously monitored for tamper (reader removed from backing plate or reader removed from wall). Tamper detection switch must be part of the reader and fit entirely within the reader housing. Use of external tamper switches shall not be acceptable. This requirement does not apply to biometric reader devices.
11. When using the vendor’s proprietary card readers, each supplied reader shall be actively and continuously monitored for communications loss by the Security Management System hardware. This monitoring shall consist of a two-way Poll-Response mechanism that insures the integrity of all signalling including LED and LCD (if equipped) data paths. Systems utilizing uni-directional “heartbeats”

or not including active, continuous monitoring of reader communications shall not be acceptable. This requirement does not apply to biometric reader devices or Wiegand card readers.

12. When using the vendor's proprietary card readers, the Security Management System shall optionally annunciate door forced and held conditions using the reader's onboard sounder, Systems that do not offer this behavior, or that require additional wiring, use additional relay outputs, or require external sounders to accomplish it shall not be acceptable. This requirement does not apply to biometric reader devices or retained legacy readers.
13. The hardware shall be made with a lead-free manufacturing process to meet RoHS requirements.
14. Communication Schemes

a. *Network Communications*

i. Field panels shall have the ability to communicate with its server or (for very large systems) its communications PC over the local or wide area network. This shall be achieved by the addition of a network interface option module (except in the case of controllers with a pre-installed network interface card [NIC]). The network interface shall support a minimum of "100 base TX" communications speed.

ii. The network interface shall support encryption utilizing AES 128 or AES 256 algorithms.

iii. Field panel models should be available to allow chains of connected panels to be created where the first panel is directly connected to the network and a minimum of 30 additional intelligent field panels daisy-chained together such that they communicate back to the single network interface.

iv. An optional modem and telephone line shall be configured to provide an alternative path for the reporting of alarms in the case of unavailability of the network. The fall back to dial-up alarms reporting shall be automatic in the event of detecting a network communications failure.

b. *Hardwired Communications*

i. The field panels shall be located convenient to the access and monitor points that they control, and shall be interconnected in a chain configuration to the server or a serial port of a convenient communications PC on the system.

ii. The system shall support a minimum of 31 intelligent field panels daisy-chained together such that they communicate back to a single serial communications port at the server / communications PC.

c. *Bi-Directional Communications*

i. A chain of field panels shall be wired in a loop configuration, by the addition of a cable from the last controller and connecting it into a second port on the PC. When this configuration is installed, should a break in the cable occur, the PC shall be able to communicate with the nodes after the break, via the secondary port. This requirement does not apply to retrofit controllers

d. *Dial-Up Communications*

i. Remote sites with field panels shall also have the ability to be centrally administered and monitored using low cost dial-up connections via autodial/auto-answer modems with each site storing all access activity for up-loading during periodic calls to update the central history log. Should an alarm occur, the remote site shall immediately call and report the incident.

e. *Secondary Dial-In Alarms*

i. Installations involving large quantities of remote dial-up sites shall have the ability to be configured with a secondary port, which is dedicated to receiving any alarms from the remote sites. This feature shall ensure that alarms can still be received even if the primary line is busy, for example, if card administration updates are occupying this telephone line.

15. Efficient Memory Management

a. *Other than Edge Network controllers, DBU Controllers shall be capable of supporting cardholder populations of at least 200,000 cards when equipped with sufficient memory, or be configured to a learning mode that allows the cards most frequently used to have their access rights stored locally in the panel's memory.*

b. *The system will include a "learn mode" function. When a card is presented which is not resident in the local panel, a verification request shall be made to the central database, if the card is valid the details shall be downloaded. If the card memory is full, the card with the oldest transaction date shall be deleted to make space for the card requested. This shall allow automatic management of cardholders, based upon frequent users having "instant" response and infrequent users learned when required.*

16. Elevator Control

a. *The system shall have the ability to provide elevator access control by (1) using a card reader to activate the elevator call button, (2) using a card* *reader in the cab to activate the correct floor selection button, or (3) a combination of both of these functions. The system shall have special field panels specifically designed to handle inputs and outputs used to interface with the elevator controls.*

b. *The panels specifically designed for elevator control shall support either a single elevator cab for up to 64 floors, or up to 4 elevator cabs for up to 16 floors each.*

c. *Each cardholder shall then have floor permissions assigned as part of the normal access rights. The system shall provide outputs to the elevator controls to uniquely verify which floors are authorized for each cardholder. The system shall be capable of tracking which floor was enabled/selected by that person.*

17. Elevator Destination Dispatch

a. *The system shall provide a two way TCP/IP based software interface between the Security Management System and the Destination Dispatch elevator system.*

b. *The system must accommodate one or more computer driven kiosks as each elevator landing lobby connected to a computer based elevator controller.*

c. *The system must display a free or secure status icon for each landing served.*

d. *The system must direct the passenger to the appropriate elevator car that was dispatched based on passenger's permission level.*

18. Database Synchronization

a. *To ensure synchronization of the distributed controllers' databases with a region's main database an internal checking process shall be provided within each controller. In the event of corruption of a controller's local database then it shall be able to detect this condition and automatically request the relevant data to be downloaded from it's local server. This action shall not require Operator intervention.*

b. *The system shall continue to provide access control functionality during this re-synchronization process.*

19. Door lock release relays shall be minimally rated for 3 A @ 30 VDC for non-retrofit controllers, 2A@30VDC for retrofit controllers.

20. Readers supporting various technologies shall provide data from card presentations or biometric authentications through a door control unit (DC) that

includes the electrical interface to the reader as well as inputs for door sensors and form C relays for outputs.

21. The DC shall support Wiegand communications to the reader. In order to provide higher levels of security, the DC shall also support bi-directional, supervised communications to the reader. Door controllers that do not support encryption and supervision of reader communications are not considered equal.

22. The system shall support an option to store cardholder biometric hand geometry templates at the panel (as part of the cardholder record). Storage of the hand geometry template data at the reader shall be unacceptable. This requirement does not apply to edge network or retrofit controllers.

23. The Security Management System hardware (except retrofit controllers and connected legacy devices) shall support all of the following options for supervision of the monitored input points:

    a. *2-state supervision – in which only secured and alarm state are indicated.*

    b. *3-state supervision – in which the input state can be secure, alarm or open circuit.*

    c. *4-state supervision – supports secure, alarm, short circuit and open circuit states.*

    d. *6-state supervision – supports secure, alarm, short or open circuit for the sensor in addition to tamper alarm and tamper short circuit states.*

24. The system shall provide the option to install Edge Network Door Controllers which support either one or two doors using PoE+ (Power over Ethernet Plus).

    a. *The intelligent PoE+ edge network controller shall provide access control processing, host functionality and 12VDC power for one or two doors (when connected to a PoE+ network port supplying maximum 802.3at power, including reader, lock, door status, request-to-exit device and auxiliary sounder).*

    b. *Each intelligent controller shall be powered using PoE, PoE+, or locally via a 12VDC supply. When powered using PoE, up to 700mA should be available for reader and electric lock power. When powered using PoE+, up to 1.5A should be available for reader and electric lock power.*

    c. *The network door controller shall provide full distributed processing of all access control functions. Each controller shall provide distributed intelligence and fast response to access requests including a minimum memory capacity of 90,000 cardholders and 18,000 offline event transactions.*

    d. *The controller shall support Flash Memory firmware infrastructure for ease of updating.*

e. *The controller shall support Wiegand output card readers and MCLP protocol for reader communications.*

f. *The controller shall provide four (4) auxiliary inputs for connection of dry-contact monitored devices. These inputs shall offer the option of 2, 4, or 6 state supervision.*

g. *The controller shall provide two (2) auxiliary relay outputs for connection of external devices.*

h. *The network door controller shall be capable of employing 256 bit Advanced Encryption Standard (AES) for all communications between the controller and host(s) system(s).*

i. *The Edge Network Controller shall provide onboard connections to a client PC via the Local or Wide Area Network.*

j. *The Edge Network Controller shall provide SNMP protocol monitoring.*

k. *The Security Management System shall provide direct network discovery and programming for the Edge Network Controller for simplified installation.*

l. *The controller shall be UL listed and conform to UL294 standards for access control systems.*

25. Retrofit Controller - Modular

a. *The Retrofit Controller shall utilize a pluggable backplane architecture allowing for new and retrofit upgrades of legacy systems.*

b. *The Retrofit Controller shall be interoperable with all other Security Management System controllers using a single Security Management System head-end software system.*

c. *The Retrofit Controller shall include an on-board cardholder database with support for up to 200,000 cardholders and up to 16,000 transactions. The database shall be maintained in battery-backed non-volatile memory to ensure that the controller will continue to operate in the event of database server or network infrastructure failure.*

d. *Each Retrofit Controller shall support a combination of up to 5 card reader, input, and output pluggable modules to support up to 16 F2F or Supervised F2F interface card readers, 8 Wiegand interface card readers, 64 monitored points, or 64 outputs.*

e. *Pluggable F2F/Supervised F2F card reader modules shall support up to 8 card readers each, with a maximum of 2 modules installed per Retrofit Controller. . The maximum wiring length between the Retrofit Controller and each F2F/Supervised F2F card reader shall not exceed 500ft. (152m),* *except in cases where existing, functioning legacy wiring and readers are being re-used, in which case this restriction shall be waived.*

f. *Pluggable Wiegand/ Supervised F2F card reader modules shall support up to 2 card readers each, with a maximum of 4 modules installed per Retrofit Controller. The maximum wiring length between the Retrofit Controller and each Wiegand reader shall not exceed 325ft. (99m) , except in cases where existing, functioning legacy wiring and readers are being re-used, in which case this restriction shall be waived.*

g. *Pluggable Auxiliary Input modules shall support up to 20 monitored points each, with a maximum of 4 modules per Retrofit Controller.*

h. *Pluggable Auxiliary Relay modules shall support up to 16 relay outputs each, with a maximum of 4 modules per Retrofit Controller.*

i. *The Retrofit Controller shall provide an integrated 10/100 Mbps Ethernet interface with selectable AES (128 or 256 bit) encryption. Additionally, each Retrofit Controller shall support communications to the Security Management System via optional hard-wired external modem or RS232 protocols. Encryption for each supplied Retrofit controller, and for the Security Management System Host software if applicable, shall be included as part of the base price of the proposal, and not as extra-cost options.*

j. *Each Retrofit Controller shall support LAN/WAN communications for up to 31 additional downstream Retrofit Controllers via serial connection to minimize consumption of network resources. This downstream communications must utilize existing wiring and terminations. Systems requiring re-termination or re-wiring of downstream chains will not be acceptable.*

k. *The Retrofit Controller enclosure shall include an integrated pre-wired tamper switch and cover lock the removable enclosure cover shall incorporate illuminated indicators allowing controller power, CPU status, and communications Status to be monitored without opening the enclosure.*

l. *The Modular Retrofit Controller shall be field-convertible between access control and elevator control functionality. This conversion shall be through settings in the host software, combined with installation of the proper I/O boards. Systems requiring a different controller type for elevator control shall not be acceptable.*

26. Retrofit Controller – 4-Door F/2F

a. *The 4-Door Retrofit Controller shall allow for new and retrofit upgrades of legacy 4 door F/2F "micros".*

b. *The Retrofit Controller shall be interoperable with all other Security Management System controllers using a single Security Management System head-end software system.*

c. *The Retrofit Controller shall include an on-board cardholder database with support for up to 200,000 cardholders and up to 16,000 transactions. The database shall be maintained in battery-backed non-volatile memory to ensure that the controller will continue to operate in the event of database server or network infrastructure failure.*

d. *Each Retrofit Controller shall support up to 4 F/2F card readers, 10 auxiliary inputs, and 8 relay outputs.*

e. *The maximum wiring length between the Retrofit Controller and each F2F/Supervised F2F card reader shall not exceed 500ft. (152m), except in cases where existing, functioning legacy wiring and readers are being re-used, in which case this restriction shall be waived.*

f. *The 4-Door Retrofit Controller shall provide an integrated 10/100 Mbps Ethernet interface with selectable AES (128 or 256 bit) encryption. Additionally, each Retrofit Controller shall support communications to the Security Management System via optional hard-wired external modem or RS232 protocols. Encryption for each supplied Retrofit controller, and for the Security Management System Host software if applicable, shall be included as part of the base price of the proposal, and not as extra-cost options.*

g. *Each Retrofit Controller shall support LAN/WAN communications for up to 31 additional downstream Retrofit Controllers via serial connection to minimize consumption of network resources. This downstream communications must utlilize existing wiring and terminations. Systems requiring re-termination or re-wiring of downstream chains will not be acceptable.*

h. *The Retrofit Controller enclosure shall include an integrated pre-wired power supply, tamper switch and cover lock, as well as provision for mounting of a back-up battery within the enclosure.*

27. Re-use of existing door wiring

a. *The system shall allow the re-use of existing wiring to door monitoring and control apparatus, without modification, rewiring, or need for additional conductors, as follows:*

i. Reuse of existing door strikes, locks, etc., and associated wiring
ii. Reuse of existing door position sensor(s) and associated wiring
iii. Reuse of existing request-to-exit sensor(s) and associated wiring

b. *Support shall be provided for at least the following types of door connections:*

i. Discrete, home-run individual wiring of lock, door position sensor, and request-to-exit sensor
ii. Discrete, home-run wiring of door lock, but a single pair loop connection of both door position sensor and request-to-exit sensor, utilizing existing loop resistances to differentiate between possible states of those sensors.

c. *Systems requiring modifications or additions to the existing door wiring, end-of-line resistors, or door sensors shall not be acceptable. Systems not supporting BOTH of the preceding methods of door sensor wiring in a single system shall not be acceptable.*

28. Enclosures and Power Supplies

a. *All electronic circuits supplied, with the exception of the Edge Network Controllers, retrofit controller, or those which are PoE powered or within a client or server or recorder PC, shall be mounted on standoffs inside the manufacturer-supplied enclosures. All such enclosures must include a key lock on a removable hinged door, and must include a tamper switch to detect when the door is opened. Systems without key locking of enclosure doors or without doors which are both hinged and removable shall not be acceptable.*
b. *All electronic circuits supplied for the access control system, except those which are PoE powered, are components of the retrofit controller, or are within a client or server or recorder PC, shall be powered by 18-20VAC through supplied 120VAC to 20VAC molded case, fully insulated isolating transformers. The transformer shall be mountable inside the supplied enclosure or separately. Systems which require 120VAC power to be brought directly to the enclosure shall not be acceptable.*

C. High Availability and Disaster Recovery

1. The Security Management System shall support a variety of High Availability (HA) and Disaster Recovery (DR) solutions including:

a. *Fault tolerant servers for 99.999% rated availability*

b. *Microsoft clustered server support for 99.99% rated availability*

c. *Remote redundancy through backup servers of general purpose nature or as in 33.1C.1.a and 33.1C.1.b synchronized through software monitoring the operation of the paired server.*

2. To provide greater client software availability, software shall be installed so that in the event of a database server failure, client machines will quickly and without operator intervention, automatically connect to a standby server machine.
3. The Security Management System product shall be capable of supporting options for 99.99% and 99.999% availability.
4. The Security Management System product shall support a disaster recovery solution using off-site database replication.

D. Encryption

1. Encryption falls into two distinct areas, firstly between clients and their Server, secondly between client and local area network panels (LAN Nodes). LAN node links shall support AES 128 and AES 256 bit encryption between the supervising client PC and its LAN Chains.
2. For client to server connections, the Security Management System shall support a solution using industry standard network cards supporting IPSec and 3DES encryption.
3. Web-based (thin client) Security Management System clients shall support SSL encryption.

E. Required Standard Software Features - The following software features shall be part of the standard product offering without requiring additional purchase or licensing:

1. The installation of the server and client software shall utilize a “wizard” interface to guide users through the appropriate installation steps.
2. The server and client software shall utilize a software-based licensing scheme. Systems requiring hardware based keys or dongles shall not be acceptable.
3. The Security Management System shall utilize Microsoft .NET architecture.
4. The Security Management System shall start up as part of the Operating System. The Security Management System server shall communicate to all clients (operator workstations and field hardware) through Windows or any other equivalent and compatible services. The Security Management System shall run as a service in the OS, and there shall be no requirement to run an application after the operating system is ready.
5. The Security Management System shall support a Graphical User Interface that minimizes training needs for even inexperienced users. The software shall include on line help displays to eliminate operator reference manuals.

6. The Security Management System software shall be run using standard x86-based hardware, and the operating system shall be Microsoft Windows or other equivalent and compatible OS as follows:

   a. *The Security Management System server shall run on Windows Server 2012 or Windows Server 2012 R2 either 32 or 64 bit or any other equivalent and compatible Server.*
   b. *Security Management System server shall support operation in a VMware ESXi environment and a manufacturer-supplied manual describing virtualization support shall be provided.*
   c. *The Security Management System client software shall run on 32 or 64 bit Windows 7 Professional or Ultimate, 64 bit Windows 8.1 Professional or Ultimate, and Windows 10 Professional and Enterprise or any other equivalent and compatible OS*
   d. *The system shall meet Microsoft requirements for "Designed for Microsoft Windows 8" or any other equivalent and compatible OS.*

7. The server shall use Microsoft SQL Server 2012® 32 or 64 bit, or Microsoft SQL Server 2014® 32 or 64 bit Standard or Enterprise database server. The system shall allow other authorized applications to gain access to the system's database should wider integration of the system at the site become a requirement.
8. The system shall use Microsoft Message Queue (MSMQ) for handling transactions between server and clients as well as between server and field hardware. Use of custom-coded or proprietary first-in-first-out (FIFO) buffers shall not be acceptable.
9. It shall be possible to select any function, within a given Operators permission, independent of the currently displayed screen. Functions will be accessed via tool bar Icons, which will include help prompts that will appear when the mouse pointer dwells on the selection button. It shall also be possible to link any standard Windows application or any other equivalent and compatible application to a custom toolbar icon.
10. The Security Management System shall support an unrestricted number of hour's definitions. An hour definition is a description of the times during a 24-hour period during which a function will be active. The system shall support a minimum of 10 intervals per hour definition.
11. The system shall support an unrestricted number of time codes. A time code is defined as a set of hour definitions – one assigned to each day of the week (including Saturday and Sunday) as appropriate, and assigned to the various types of holidays (exceptions) defined in the system.
12. The system shall support a minimum of 9 holiday types. A holiday type shall be assignable to an unrestricted number of dates on the calendar.
13. Operator Permissions

a. *System operators shall be associated with a log in Name and Password. A system option will determine whether strong operator passwords will be used. The minimum definition of a strong password shall be a password that contains at least one upper case character, one lower case character, one numeral and one punctuation mark, with a minimum password length of six characters. Additionally the password cannot contain any full word of the operator's username.*

b. *The option to use a Secure Biometric or Smart card for system logon shall be provided. When used, this option will force the operator to present their Name, Password and Biometric or Smart card.*

c. *The operator's account shall be role based. The role is a permission profile. This will determine the functions that shall be available to that operator when logged-on to the system. The system shall support an option to hide Personal Identification Numbers of cardholders when an operator is viewing a record.*

d. *The system shall show each operator only features and options for which he or she is authorized. Features and options for which the operator does not have permission must be hidden. Systems that display functionality that is unavailable due to inadequate permissions shall not be acceptable, even if such functionality is disabled or "grayed out".*

e. *Card record data entry shall be divided into operator permission areas, allowing separate permission categories to be assigned for the viewing of personal data, ID badge printing and access right management.*

f. *The Security Management System shall support an unrestricted number of operator accounts and operator roles.*

g. *For all operators, a means of re-arranging their Icon tool bar shall be provided to allow the most frequently used Icons to be repositioned by the operator.*

h. *The system shall store operator preferences based on logon information. This feature shall allow an operator to work with their preferred configuration independent of which workstation they occupy.*

i. *The system shall support an option to reset all window layouts to a pre-defined "Home Screen".*

14. Video Badging

a. *The system shall incorporate video imaging as a fully integrated function within the SME to customize access control cards by printing an identity badge directly onto the card. The badge design and image capture capabilities shall combine with the latest technology card printers to allow* *the production of an ID badge pass for each card holder at the time of registration.*

b. *For each cardholder both a facial image and a signature shall be able to be captured, or imported, and stored within the database as part of the card record. These images shall be captured from a supported USB webcam or standard CCTV camera connected to the computer, or imported if available as a bit map or JPEG file. The system shall use data compression techniques to ensure efficient use of the available hard disk space to maximize the number of images that can be stored on the hard disk.*

c. *Alternatively, system shall support use of an Axis IP camera with available utility to act as a badging camera. Any Axis IP camera in the system may be utilized.*

d. *System shall provide the ability to crop the image (live capture or imported from JPG, BMP, or WMF) to the desired area maintaining the proper aspect ratio.*

e. *Additionally, a signature may be imported from a signature capture terminal connected to the system via an RS-232 com port or USB port of the client PC local to where the card is being issued.*

15. Badge Design and Printing

a. *A comprehensive integrated badge design facility shall be provided as a standard integrated feature of the single Security Management System software application, with no separate licenses or license fees required to activate the feature. The badge designer must allow an unrestricted number of custom badge layouts to be defined, and then saved with a suitable description as a reference. This shall make full use of the card record details such as name, card number, inactive date as well as allowing personal data to be included in the badge design. Company logos shall be imported as bitmaps (BMP) or JPEG images to provide a personalized corporate appearance to the card.*

b. *All elements incorporated into the design shall be able to be rotated.*

c. *Badge design within the Security Management System shall contain either single sided or double-sided designs. Each side of the card may also be designated as being blank, or magnetic stripe side, or smart chip side, to ensure the designer is aware of the available space where printing may be incorporated for each card combination. The badge designer function shall be capable of supporting portrait, landscape, standard and custom-sized card designs.*

d. *When creating a new card record a badge preview screen shall also be included that displays the specific card's details on the selected badge design to allow confirmation prior to requesting the badge to be printed.*

e. *Each new cardholder record shall have the option to be flagged for future printing. Cards flagged in this manner shall be easily recalled at a later stage and processed for output to the printer in a single action. Selecting multiple cards for bulk printing shall also allow each card to be printed either with its specific badge design, as defined within each card's record, or alternatively printed with a selected common badge design. Encoding of magnetic stripe cards shall also be included as part of the bulk printing process.*

f. *The Security Management System shall support any manufacturer's ID badge printer with a Microsoft Windows or any other equivalent and compatible services (depending on the workstation configuration) compatible printer driver.*

g. *The Security Management System shall incorporate the option to encode a magstripe or smart card during the print cycle. Applications that require on-site encoding can combine both actions in a single process. Encoding may only be supported on a limited set of printer models defined by the Security Management System manufacturer.*

h. *Each badge design shall include a default printer and validity period.*

i. *Badge Designs shall include the ability to add access rights to the badge design, so a cardholder issued with a specific badge design will automatically receive badge permissions related to that badge design.*

j. *The badge designer shall support the ability for objects (images, or other fields to be printed to the card) to be enabled or disabled by the presence of a specific label in the cardholder record. For instance, a logo indicating a certain training would be printed only if the personal data field identified indicated such a certification for that cardholder. Solutions requiring a separate badge design for any change in badge graphical content shall not be acceptable.*

k. *Printing and supply of 150nos. of photo identity cards, **as and when required**, as per the details provided (photo & other details) by the Embassy.*

16. Identity Verification

a. *Identity verification shall include the ability to monitor up to 9 lanes, and each lane shall comprise a single entry point.*

b. *There shall be up to three live video camera views available per lane on the same window to verify that each card offered is in fact being used by* *the person to whom it was issued. (for monitoring vehicles approaching and arriving at the entry point of each lane for example).*

c. *A method of granting access to the individual at each entry point with a single mouse click shall be provided.*

d. *Each lane shall automatically display the stored image for a card when used at a reader.*

e. *The operator shall be provided with a means to quickly search cardholder records by name to manually compare and verify basic card information.*

f. *Each lane shall provide configurable cardholder information to be displayed when a card is presented at the entry point reader (for example card expiry date and personal data)*

g. *This screen shall also be frozen and printed to provide a hard copy evidence of any abuse observed by the operator. For high security entry points, the system shall be configured to not grant access until the operator has verified the stored and live images are the same person, with the door release being controlled by the system operator.*

h. *This screen shall provide manual operation of pre-defined commands as a means of rapid response to events for each lane.*

i. *Intercom station call and answer functionality shall be provided for each lane.*

17. Report Generation

a. *Extensive history reporting shall be a standard integrated feature; and shall include the ability to review all system alarms, access control activity, and operator actions. These reports shall be made available for review via the operator's display screen, or to a printer, or to another disk media. Extensive sort parameters shall include by any of the "Personal Details" fields or Titles, for example by "Department", and only Names commencing with "SM*".*

b. *The system shall support generation of reports detailing the system operation. The following reports shall be available in the software:*

i. Cards on site
ii. Hours on site
iii. Cardholders with access to each door
iv. Access rights of each cardholder
v. System Configuration
vi. Scheduled and Conditional Commands defined
vii. System operator transaction history

c. *It shall be possible to replay video clips associated with events by directly interacting with the report as published to the computer screen.*

d. *The system shall demonstrate the ability to export data, for example reports, to other standard office word processing packages such as Microsoft Word®.*

e. *The system shall provide system management reporting, including detailed listings for all the operator actions and the current cardholder database for output to the display screen, printer or disk media.*

f. *The system shall have the ability to save frequently used report configurations and associate them with a "Title". Such predefined reports shall be available from a list to simplify the report selection. It shall be possible to request these reports to run immediately or schedule them to occur at a specified date and time.*

g. *Scheduled reports shall additionally have the option to be automatically repeated by specifying the number of days and reporting period to be included, for example a weekly report of Alarms to run at 10:30 am each Monday and including the previous 7 days of Alarms.*

h. *The system shall allow custom reporting options by providing an interface to a commercially available 'off the shelf' reporting product, such as Crystal Reports. The interface shall present all database fields in a structured format, which does not require detailed knowledge of the database design and table relationships.*

i. *History Reporting*

i. Extensive reporting shall be included to provide the ability to review all system alarms, access control activity and operator actions. These reports shall be available for review on the operator's display, to a printer, or to a file.

ii. Extensive sort parameters shall include any of the personal details fields of information such as by department, job title, vehicle registration, contractor company name or any other reference appropriate for each site.

iii. Frequently run report configurations shall be saved allowing them to be selected and run on demand, or scheduled to run automatically as required. When scheduled to run automatically this shall have the ability to be repeated.

iv. Total Hours Spent On-Site: This report shall provide a detailed audit of the arrival and departure times for cardholders and calculates the total time spent on site for the chosen reporting period. This report shall be filtered by any of the personal data fields of information associated with each cardholder.

v. Cards On-Site Reporting: This report shall provide a list of cardholders currently on the site. This may be for all persons within the site or just who, for a particular department or a particular contractor company, is currently present. The report may also be run to cover just a part of the site, for example, cardholders in a particular building or room.

vi. Report Auditing/Archiving: The Security Management System shall have the option to automatically and without user intervention keep a separate archival copy of each generated report, whether the report is sent to screen, printer, or file. The archival copy must be generated at the time of each request and stored unmodified thenceforth. Systems that attempt to reconstruct the archival copy only when it is requested are not acceptable.

18. Client PCs

a. *The system shall support an unrestricted number of client PCs to suit growing enterprise requirements. The system shall provide the means for multiple operators to simultaneously administer the system from convenient locations connected via a local area network (LAN) or across a wide area network (WAN).*

b. *Systems that operate on the SQL Express database server that restrict the number of clients shall be upgradeable to a fully unrestricted version of the software.*

c. *Clients shall not use mapped drives for server connections.*

d. *Clients shall not use UDP messaging.*

e. *System shall support a minimum of two pc monitors per client. The system shall additionally store the last position and size of all open dialog boxes and screens upon exiting the application on a per operator basis. The next time the operator logs into the application, the screen positions shall be restored. Such operation shall be independent of which workstation the operator uses.*

f. *The capability shall be provided to "lock" the window arrangement for each operator individually, such that each time they log on they have a fixed arrangement of windows or any other equivalent and compatible services that they do not have the ability to alter. Systems that cannot prevent an operator from closing or rearranging windows will not be considered. Systems that allow windows to be locked by workstation but not by user will also not be considered.*

19. Addition of Cardholders to the System Database

a. *The system shall provide a means of assigning access control rights to each cardholder. Access control rights determine which access points are accessible to the cardholder based on date and time of day. The system shall support an unrestricted number of access rights.*

b. *The software shall also provide the ability to assign an advanced set of Access rights to a cardholder on a temporary basis. The change may be initiated at any time by an authorized operator, or automatically between specified dates. This shall provide the facility of automatically adding to a card's rights between a specified date range, after which the card will revert to its normal Doors and Times. Advanced access rights shall be able to be configured for multiple date ranges.*

c. *Each cardholder shall either be associated with standard door timings for door release, door open and door pre-held, or be given extended timings for persons with disabilities or – for example - someone who has to push a cart.*

d. *Cardholders who have not used a card reader for some time shall be readily listed to allow their card's status to be reviewed. An additional feature shall allow cardholders to be automatically set inactive and therefore access would be denied should the card have not been presented at any reader on the system for a defined number of days.*

e. *Cardholders shall be assigned an expiration date, and more specifically an expiry time, after which a card shall automatically become inactive and therefore be rejected at all readers on the system. To further simplify card administration, the system shall have the ability to be configured to automatically purge expired cardholder records after a configurable number of days from the date of expiration.*

f. *Cardholders who have mislaid or forgotten their issued card(s) shall be provided with a means of temporary card assignment. All cards issued for the cardholder shall automatically be inactivated whilst the temporary card is active.*

g. *The system shall allow for the definition of Access control rights to be associated with a badge design. Each user that selects that badge design shall be provided with the associated access control rights that can further be customized for the specific cardholder.*

h. *The system shall allow access control rights to be defined for a cardholder on a per reader basis. A timecode will be associated with each reader as it is assigned to the cardholder's access control rights.*

i. *The system shall allow access control rights to be defined for a cardholder on a per reader group basis. Reader groups are groups of readers. A* *timecode will be associated with each reader group as it is assigned to the cardholder's access control rights.*

j. *The system shall allow access control rights to be defined for a cardholder on an access code basis. An access code is a group of access control rights combining different readers and different reader groups, each at different timecodes. This is to be particularly suitable for role based access right assignment.*

k. *The system shall have a note field associated with each cardholder record. The note field shall be free form text and shall support a minimum of 256 characters. The note field shall further support the ability to attach multiple files (of any type or size) to each cardholder record.*

l. *When viewing a cardholder record the last twenty-five (25) valid door access transactions shall be displayed to help locate a cardholder.*

m. *A driver's license scanner shall be supported to simplify data entry of cardholder information. The scanner support shall include, at a minimum, the ability to automatically read, through optical character recognition, the most common fields from valid driver's licenses issued by all 50 states in the USA and from international drivers licenses, and populate these fields into the appropriate user-defined personal data fields in the cardholder record.*

n. *The system shall support a field for assigning an approving official to the cardholder record that defines the individual who authorized the assignment of a credential. Approving officials shall have an associated validity period and image of their signature. As an option, the assignment of an approving official shall be mandatory.*

o. *The Security Management System shall allow the user to enroll biometric data as part of the cardholder enrollment process. The number of verifications to determine applicability of the enrolled biometric data shall be configurable.*

p. *The Security Management System shall obtionally be connected to other suitable biomertric systems and the cardholder name and card number shall be passed to that other biometric system by a standard mechanism which has been cionfigured by the biometric system manufacturer.*

20. Cardholder Details

a. *Cardholder information shall include first and last name, card number, PIN code and valid period to provide automatic expiration. PIN numbers shall be configurable from 4 to 8 digits in length.*

b. *Each cardholder record shall also incorporate at least 50 user-defined personal data fields, independent of user-defined fields for visitor management.*

c. *Data entry shall be simplified by remembering previous entries of personal data and allowing selection from a pick list to minimize repetitive typing when creating each cardholder's record. The cardholder database and the history log shall also be sorted by any of the additional fields of information making them a powerful tool for filtering data.*

d. *Personal data fields shall support free entry text, picking an entry from a previously configured list, or picking an entry from an updatable list. Each of these entries shall further be categorized as a date, a time, general input, card inactive date or customized input. Each category shall support the masking of input data to assure data integrity. For instance, a date mask might look like "mm/dd/yyyy" to indicate that the date input should be a two-digit month followed by a two-digit day followed by a four-digit year all separated by the slash character. The mask shall be required for customized input.*

e. *Personal data fields shall have the option of being configured as mandatory.*

f. *Personal data fields set as dates shall be definable so as to make badges expire when the date is reached, where the dates are dates at which specified training or other compliance expires*

21. Locator

a. *This feature shall provide a quick method of locating cardholders by displaying the last 25 valid history events along with the time, date and access point used. This information shall be available for an individual or group of persons by name, card number or by personal data.*

22. Card Watch Feature

a. *Any cardholder shall be easily tracked as they move around a large site by selecting card watch. As the person uses their access control card, the system shall have the ability to automatically notify the operator of the person's presence at each location.*

23. Key Card Mode

a. *Key card mode authority shall be assigned to special cardholders, such as site key holders, and can be enabled on a per reader basis. This shall* *allow a person when vacating an area or building to change the reader's mode of operation from normal access control to Key Card Out operation.*

b. *When in this condition only persons with key card privileges shall gain access through the door, all non-key card users are rejected regardless of their card's current access rights.*

c. *This special feature shall be activated/deactivated by the key cardholder, using a card swipe followed by a special code entered via the reader's keypad.*

24. Serial Device Interface

a. *The software shall allow the definition of ASCII commands to be sent out over a computer serial port (physical or virtual) or through the RS-232 interface of the DBU. These serial commands shall be available through the user interface as well as in the conditional logic described herein.*

25. Automatic Holiday Override

a. *The software shall be programmed by the operator to recognize special or holiday dates, which in turn can be linked to operational changes in how the site is to be managed on these specific days. This feature shall notify a system operator of individual holiday dates up to seven days prior provides a useful check on the date's current validity. Multiple types of holiday dates shall also be provided so that partial days or early closing requirements on specific dates can be accommodated.*

b. *Cardholder definitions shall be provided with the ability to add vacations in a quick and convenient manner. Dates and time periods shall be defined during which access is denied to all access points and an alarm generated if access is attempted.*

c. *The Security Management System shall provide a calendar function to enable scheduling of events up to three (3) years into the future.*

d. *The Security Management System shall provide the ability to schedule one-time events for up to three (3) years into the future.*

26. Multi-Company System Partitioning

a. *The access point readers, monitor points, and auxiliary outputs shall be managed on a multi-company partition basis by simply defining which devices are to be included in a partition.*

b. *The Security Management System shall be supplied with the ability to manage up to 64 partitions, and shall have an option to manage up to 999 partitions.*

c. *Multiple private or public entities shall be able to share the system with database segregation for card records and ownership of readers, monitor point inputs and switching outputs dependent upon the operators assigned permissions. Each company partition shall allow for autonomous system administration, allowing partitioned card administration, reports, and alarms.*

d. *Operator permissions shall be created and assigned globally or by the owning company. When created and assigned globally an Operator's password shall be associated with one or more companies.*

e. *Alarm reporting shall be routed to a client PC located at the company owning the monitor point or reader and can be automatically redirected to a different PC at pre-programmed times and selective days of the week.*

f. *Common areas, such as the main entrance, shall have the ability to be shared so that all companies may access these doors, even when different card customer/site codes have been configured.*

27. Alarm Management

a. *Alarm and activity management must be handled in the same executable program as other access control functions such as cardholder management, badging, and hardware configuration. Systems utilizing a separate application for alarm handling shall not be acceptable.*

b. *Alarms must be displayed in a separate window from non-alarm system activity. Systems which display both alarms and non-alarm activity in a single window shall not be acceptable. It must be possible to display either the alarm window, the activity window, or both at any time.*

c. *The Alarm window shall provide a method to filter alarms for all available alarm field parameters. Configured filters shall be saved per user with the option of sharing to all users. Filtered records shall be displayed in a separate view within the alarm window.*

d. *The system must provide separate permissions for alarms and activity, and allow users to be individually granted rights to view and or process either, neither, or both. Systems which cannot separately grant privileges for alarms and for non-alarm activity shall not be acceptable.*

e. *Alarm handling shall be efficiently managed with up to 999 priority levels and user definable instruction messages to ensure the operator monitoring the site takes appropriate responses.*

f. *To provide additional information when reviewing alarm signals, the operator shall either enter custom comments or simply select from a predefined pick list to provide a time-stamped record of all the actions taken throughout the incident.*

g. *Predefined manual commands shall be uniquely assigned for each alarm, and readily activated by the operator via a command button provided on the alarm acknowledgement screen. Additionally automatic trigger commands shall be configured to automatically operate in response to any given alarm condition.*

h. *The Security Management System shall be optionally configured to require operator comments when acknowledging alarms.*

i. *The Security Management System shall support the ability to selectively choose alarms to acknowledge and/or clear.*

j. *Each alarm shall be configurable to have a specified user defined color and sound, using standard sounds provided with the system or custom generated multimedia wave files.*

k. *Each alarm shall be capable of linking video from specified integrated video management systems (if applicable) for incident playback.*

l. *The Alarm Monitor screen shall provide an indication that cardholder information is available for a specific alarm. A "Card" button shall be available that when pressed will display the cardholder badge image.*

m. *Alarm monitor screen shall support the display of alarm statistics, shall provide up to ten alarm filters to be displayed in different tabs on the alarm screen, and shall provide the ability to sort based on each different column.*

n. *It shall be possible to add additional relevant fields of information to the alarm monitor screen*

o. *Each alarm shall be time-stamped in the local time zone (not the server time zone), and the system shall support the additional display of labels associated with different geographical time zones such as PST, EST, GMT, etc. The labels for time zones shall be customizable.*

p. *The system shall permit the routing and display of real time activity at any standard client PC. Activity shall be shown in a dedicated activity window that is updated automatically when new transactions occur. This option shall not be limited to routing transactions to one location and shall support the simultaneous routing and display of real time activity at multiple locations.*

q. *The activity display refresh near real-time and shall allow filtering, color coding, addition of cardholder photos to relevant events, freezing of the* *display and review of historic activity for any previous date where the activity is still in the database.*

r. *Alarms shall be capable of being routed to specific client machines by time of day or day of week.*

s. *Unacknowledged alarms shall be capable of being routed to alternate client PC(s) or to be sent by email based on age and priority of alarm.*

t. *E-mail alarm messages shall be controlled by time of day and day of the week. For example, e-mail to the Facility Security Supervisor would only be generated when alarms occur during after-hours times.*

u. *Each alarm definition shall allow a destination e-mail address to be defined. The e-mail address may be an address group as defined in the e-mail MAPI application.*

v. *The display of reader door alarms shall be automatically enabled or disabled by the use of timed commands, either by reader or by a group of readers.*

w. *The system shall support a generic ASCII input capability that allows the system administrator to define specific ASCII input strings as alarms to be displayed in the alarm monitoring window as well as on the graphical map interface if so configured.*

x. *An optional advanced alarm workflow capability will be available providing alternative routings through the alarm processing based on the answers to questions provided by operators. The workflow capability will be configured through an integrated dataflow diagram style drag and drop configuration screen*

28. Task Management

a. *A method to allow any ad-hoc or regular tasks to be completed by operators shall be provided.*

b. *Tasks shall define actions to be completed by specific users, or any user with a specified user role.*

c. *Each task shall be assigned a due date and time, and if the task is not marked as completed before the due time is reached its status shall automatically change to 'overdue'.*

d. *The tasks selection window shall show all completed and incomplete tasks, each task displaying subject, due date and time, the user name or role that the task is assigned to and current status.*

e. *The tasks window shall provide filters for viewing task records and the ability to add new tasks, or open existing tasks (to mark them as complete or add comments for example).*

f. *Tasks shall allow alarm generation when they become overdue or on the immediate creation of a new task.*

g. *It shall be possible to add details to each task (for example, how to complete the task) and comments to facilitate management.*

h. *Tasks shall be configurable for re-occurrence (for example every Tuesday or every day). Once the task is completed a new instance of the task shall be created.*

i. *A means to attach files to tasks shall be provided.*

j. *Overdue tasks appearing in the alarm window shall be cleared by opening the alarm and selecting 'complete'. If the task is configured as 're-occurring' a new task shall be generated depending upon the settings in the tasks recurrence window tab.*

k. *Completed tasks shall be deleted automatically after the period specified by the 'Purge daily logs after' value configured for the Security Management System.*

l. *The number of unacknowledged task alarms shall be displayed in the Security Management System status bar along the bottom edge of the main window -a blue background shall distinguish them from system alarms.*

m. *The task Manager shall be a standard feature of the Security Management System with no separate licenses or license fees required to activate the feature.*

29. Graphical Site Maps

a. *To further enhance the presentation to the operator, the system shall have the ability to import and use graphical maps. Graphics shall be linked together using a tiered tree structure. To speed the location of an incident, each map level shall contain a clearly visible indicator as to which sub map the operator should select next to find the device that is in alarm.*

b. *Graphics shall also have the ability to be configured to appear automatically on presentation of a new alarm, providing the operator with prompt visual indication that an alarm has occurred.*

c. *The status of card readers, doors, monitor points and auxiliary outputs shall be requested from any graphic by simply selecting the icon representing the device and its current state will be displayed.*

d. *The icons on the graphic map shall dynamically indicate the status of the device they represent. For example, a door icon shall change to show the door open when the door position sensor indicates such, and shall change* *to the original icon when the door is again secure. Additionally, monitor points shall also change to show their current state.*

e. *Should the operator wish to change the current setting, simply pressing the right mouse button shall cause the appropriate command options list to appear for selection.*

f. *Having selected a command, confirmation shall be provided by reflecting the change in status on the display.*

g. *It shall be possible to import photos, graphics and drawings in the following formats: JPEG, Bitmap, Windows metafile or DXF or any other equivalent and compatible format .*

h. *Icons representing access points, monitoring points, switching outputs, alarm inputs, cameras or intercom call stations shall be placed on any map at the required location in a drag and drop manner.*

i. *It shall be possible to define on the graphic the location of card readers, access doors, alarm monitored points, output switching relays, cameras, intercom call stations and alarm panel devices.*

j. *The graphic display shall allow the operator to view the video stream from any video camera defined on the security management system. The graphic display shall allow the display of stored Digital Video Clips.*

k. *It shall be possible to define on the graphic the location of reader groups and camera groups. Such groups shall be placed and appear as a single icon, but actions taken on them shall affect the entire group.*

l. *It shall also be possible to change the status of card readers, reader groups, floor groups, alarm monitor points or output switching relays and confirm the successful execution of such commands from the graphical display. This functionality shall be capable of being restricted per device based on operator permissions.*

m. *The graphic display shall include the option to display a group of similar devices as a single icon. Once devices are grouped it shall be possible to change their status. For example, it shall be possible to unlock all entrance doors by executing a single command from the map display.*

n. *It shall be possible to display a device on any graphic, on multiple graphics, or on no graphics. It shall also be possible to display the same device in multiple locations on the same graphic. Systems that do not allow devices to be placed multiple times on the same or multiple graphic shall not be acceptable.*

30. Manual and Automatic Commands

a. *Operators shall be provided with a wide choice of manual commands embracing the control of card readers, monitor points, output switching relays and door locking devices. Also the operator shall have the ability to check the status of single, or multiple devices. This shall ensure the operator is always able to check the operational status of the system and make any adjustments as requirements change. When graphical maps are utilized, status requests shall be simply initiated by "clicking" on the device icon within the map. This functionality shall be capable of being restricted per device based on operator permissions.*

b. *Automatic commands shall be included and may operate on a timed or event basis.*

c. *Scheduled commands shall easily be defined linking complementary commands to occur at the start and stop times of any chosen timecode.*

d. *Event triggered commands shall provide an extremely powerful means of creating IF/THEN/WHEN associations encompassing a wide selection of IF conditions to the automatic execution of THEN commands subject to a WHEN timecode being active. A minimum of 10 THEN actions shall be available per trigger command.*

e. *Devices shall be managed on a partition basis by grouping card readers, monitor points and auxiliary outputs. This feature shall allow multiple devices to be actioned by a single command when using manual, timed and conditional commands. This functionality shall be capable of being restricted per device based on operator permission.*

f. *The Security Management System shall support an unrestricted number of automatic (scheduled and trigger) and manual commands. These commands shall be capable of spanning across multiple field controllers.*

g. *Triggered commands shall be executed directly within field controllers if the input initiating the command and the output of the command are held within the same controller.*

31. Card Initiated Commands

a. *The software shall allow authorized cardholders to initiate powerful trigger commands manually from selected card reader locations when certain models of card readers are used in conjunction with the field panels.*

b. *Up to 99 predefined commands shall be invoked by an authorized card allowing, for example, a patrolling guard to switch on outputs, disable monitor points, lock doors, providing remote management of the system during a patrol of the site.*

c. *The system shall only permit assigned users to enter command codes at keypad readers. Such assigned users shall not be restricted as to when or where they can enter a command code – such restrictions may be placed on the commands themselves.*

32. User Code Mode

a. *The Security Management System shall support the ability to put a keypad-equipped reader into User Code Mode. This feature shall allow a cardholder to gain access by entering the card number of a valid card at a reader keypad, therefore not requiring the holder to carry a card.*

b. *User code mode shall be enabled on a per reader basis and this mode shall support card number only, or card number and its assigned PIN code.*

33. Visitor Management

a. *Visitor Management shall be incorporated as a standard feature of software, with no separate licenses or license fees required to activate the feature. Operators shall be able to pre-enroll visitors using a Web (thin) or Standard (thick) client. The thin client shall connect to the server via thin client technologies such as Citrix and Microsoft™ Internet Explorer to permit any operator with visitor permissions assigned the ability to pre-enroll visitors without the need to install client software on their local machine.*

b. *Visitor Management shall be fully integrated with other key areas of the system, such as access, alarms management, muster and Video ID Badging. Visitor records shall have 50 personal data fields with user definable data titles independent from the personal data fields defined for cardholders. All visitor transactions and movements shall be recorded and may be reported on and filtered, using the extensive reporting capabilities of the software. Visitors may exist without being assigned a card number if access control is not required.*

c. *Data entry shall be simplified by remembering previous entries of personal data and allowing selection from a pick list to minimize repetitive typing when creating each visitor's record. The cardholder database and the history log shall also be sorted by any of the additional fields of information making them a powerful tool for filtering data.*

d. *Personal data fields shall support free entry text, picking an entry from a previously configured list, or picking an entry from an updatable list. Each of these entries shall further be categorized as a date, a time, general input, or customized input. Each category shall support the masking of* *input data to assure data integrity. For instance, a date mask might look like "mm/dd/yyyy" to indicate that the date input should be a two-digit month followed by a two-digit day followed by a four-digit year all separated by the slash character. The mask shall be required for customized input.*

e. *Personal data fields shall have the option of being configured as mandatory.*

f. *Visitor time of arrival and time of departure shall be tracked by the system. This feature shall be available even if a visitor is not issued a card or card number in the system.*

g. *It shall be possible to configure a reader to automatically inactivate presented visitor cards ready for reuse.*

h. *The system shall support a driver's license scanner including optical character recognition to ease data entry.*

i. *The Security Management System shall support capture of a business card image.*

j. *The Security Management System shall support the inclusion of a custom message for each visitor record.*

34. Area Occupancy Monitor

a. *The system shall include the ability to monitor the occupancy of an area.*

b. *Occupancy thresholds shall be configured for the maximum and minimum values, and associated with automatic conditional commands. These shall be used for applications such as to disable the entry readers when all the garage spaces are occupied and switch a garage full indicator sign on.*

c. *Complementary commands shall also be provided to enable the entry readers and turn off the indicator as a vehicle leaves the garage. Similarly when the garage is empty, the lights could be automatically turned off.*

35. Device Configuration

a. *The system shall support a notes field to be associated with each device configured on the system. The notes field shall be free-form text, and shall support a minimum of 256 characters. The notes field may be used for detailed device descriptions or for maintenance history.*

b. *The system shall allow a unique set of arbitrary files of any type to be associated with each device.*

c. *The system shall provide a hierarchical tree view of the system configuration supporting expansion and collapse of any and all branches.*

d. *It shall be possible to define the location of each device (card reader, door controller, camera etc.) within the system through a dedicated location field in the configuration record.*

36. History Archive and System Back up

a. *The system shall be capable of retaining at least 25 years of activity in its online log file, disk storage space permitting. Systems that require offline storage of historical events shall not be acceptable.*

b. *The system shall allow on line archiving of history logs, along with database back-up of system configuration and cardholder details. To further ease the burden of remembering to back up your system's database, this function shall be able to be automated to occur without intervention at a pre-set time.*

c. *The system backup and history archive shall be to a local or remotely accessible UNC path.*

37. Support for Smart Cards and Biometrics

a. *The system shall have the integrated capability to capture at least two forms of biometrics – preferably fingerprint and hand geometry.*

b. *Any proposed fingerprint solution shall support the enrollment and use of at least two fingerprints, which shall allow the cardholder to present either finger to gain entry.*

c. *On a timed or manual basis the system shall be configurable to allow entry using the smart card only, smart card plus fingerprint or smart card plus two fingerprints, thereby raising or lowering the level of security as required.*

d. *The system shall allow the assignment of a fingerprint for normal entry and a different fingerprint for duress entry. The cardholder shall have the ability to trigger a silent duress alarm by presenting the duress fingerprint. This provides the cardholder with a safe way to indicate a duress condition, without alerting anyone locally that the alarm has been triggered.*

e. *An option to recall the fingerprint acceptance threshold from the smart card to override the threshold stored at the reader shall be provided. By recalling the threshold from the smart card, overall site security is not compromised by a poor quality fingerprint, which would normally require a low acceptance threshold to be set at the reader.*

38. Server Hardening and Cyber Security

The manufacturer of the Security Management System shall make available documentation on Server Hardening, which shall, at a minimum, detail the TCP/IP ports that are utilized by the system to allow other ports to be closed.

39. Anti-Passback

a. *The system shall support both "hard" anti-passback and "soft" anti-passback alarm reporting modes.*

i. If the cardholder has access rights at a reader, but creates an anti-passback alarm, if the reader configured as hard anti-passback sends an anti-passback alarm and denies access to the door/portal.

ii. Soft anti-passback sends an anti-passback alarm, but still allows access through the door/portal.

b. *The system shall support timed anti-passback. The principle of timed anti-passback is simple: once a card has been used at a timed anti-passback reader, the card causes an anti-passback violation if it is used again at the same or another timed anti-passback reader within a predefined period of time. The exception to this rule is when the anti-passback reader has been defined to be for an exit route. In this case, the card can be used at any time without causing an alarm or event. This allows for situations where a person enters an anti-passback-protected area, then wishes to exit the area immediately, perhaps, for example, because he or she forgotten something.*

c. *The use of an exit anti-passback reader also causes the time delay for reuse of the card to be zeroed, so in the example, the person can re-enter the antipassback-protected area immediately, without having to wait. The delay can also be zeroed from the Card Holders screen or by means of an antipassback command. Sending a command may be useful if, for example, people have passed through an exit during a fire drill and the delay is long.*

d. *The system shall support zonal anti-passback. In the case of zonal antipassback, the building needs to be partitioned into zones. For example, zone 1 may be the main lobby, zone 2 the computer room, etc. For each reader that is defined as a zonal antipassback reader, you can specify which zone of the building the card is going from and which zone it is* *going to. For example, the reader may allow a card to go from zone 1 (e.g. main lobby) to zone 2 (e.g. computer room).*

e. *The system shall remember which zone each card is in and update this information whenever the card is used at a zonal antipassback reader. An antipassback alarm or event is generated if the reader's from zone does not match the card's currently-recorded zone. For example, an alarm or event is generated if the from zone of the reader is zone 3, but the card is currently recorded as being in zone 1. If a card's currently-recorded zone and the actual zone get out of step, either because of some violation of the system (e.g. a person has previously climbed over a turnstile) or for a legitimate reason (e.g. a person has passed through a fire exit during a fire drill), some means is obviously required to bring the two back into step. This can be accomplished from the Card Holders screen or by means of an antipassback command. Both methods put the card(s) into a "neutral zone", so that the next transaction at an antipassback reader is always accepted without violation, and the reader's to zone becomes the card's new zone.*

40. Elevator Control

a. *Each cardholder shall have floor permissions assigned as part of the normal access rights. The system shall provide outputs to the elevator controls to uniquely verify which floors are authorized for each cardholder. The system shall be capable of tracking which floor was enabled/selected by that person.*

b. *The system shall be capable of integrating with elevators through a relay based field controller and also through a software based destination dispatch system according to the requirements of the project.*

41. Data Connect Option

a. *The system shall provide an option to import and/or export both cardholder details (including facial images and signatures) and system alarm information to/from an external source. This option may be used to speed initial commissioning of the Security Management System's database, or in some cases, to allow synchronization with other employee management systems. This option may also be used to pass common data to other employee-related systems or databases. It shall be possible to manually start or schedule the data import. It shall also be possible to start the data import process from an external application, thus providing the means for real time import.*

b. *The interface requirements shall be fully defined and support either a comma delimited ASCII text file or a Microsoft SQL® database import mechanism. Fully detailed supporting documentation shall be provided to enable a third party to design and implement this facility without needing reference to the system's manufacturer.*

c. *Imported data shall reside in an intermediary table within the database until an integrity check can be applied. Only after satisfying this test will data be included in the Security Management System data tables.*

d. *The data connect option shall be provided without extra charge for Enterprise sized Security Management Systems.*

42. XML Developers Toolkit Option

a. *The system shall support the ability to send and receive commands to/from external web services through an XML interface, the XML Developers Toolkit. All operations through this interface shall be accompanied by a logon username and password that will be associated in the Security Management System with operator privileges, which will limit what is permissible. The interface shall use standard security provided by web services.*

b. *The XML Developers Toolkit shall support the import of cardholder details. An external software system may use web services, for example, to add new cardholders, delete cardholders, modify existing cardholder data, make cards inactive, and change access rights.*

c. *The XML interface shall allow an external software system to obtain the details of cardholders that are already in the Security Management System database.*

d. *The XML interface shall allow an external software system to view, acknowledge, and clear outstanding Security Management System alarms.*

e. *The XML interface shall allow an external software system to send a command to a device already defined in the Security Management System (e.g. to open a door or display video from a network camera).*

f. *The XML interface shall allow an external software system to view the status of an Security Management System device (e.g. to determine whether a door is locked or unlocked).*

g. *The XML interface shall allow an external software system to import alarms from external equipment, such as intrusion systems.*

43. Smart Card Encoding Option

a. *The system shall provide the ability to encode contactless smart cards with access control information. The system shall support encoding either MIFARE or DESFire.*

b. *The software shall support the NXP Pegoda, GemPlus, and the HID OmniKey CardMan contactless card readers for the encoding and reading of Mifare and MIFARE DESFire cards.*

c. *The system shall be capable of capturing fingerprint biometrics and storing them on a contactless smart card, which will then be read and used to verify the cardholder during an access control transaction.*

d. *Any proposed fingerprint solution shall support the enrolment and use of at least two fingerprints, which shall allow the cardholder to present either finger to gain entry.*

e. *An option to store the fingerprint acceptance threshold in the smart card or at the reader shall be provided. By storing the threshold in the smart card, overall site security is not compromised by a poor quality fingerprint, which would normally require a low acceptance threshold to be set at the reader.*

44. Guard Tour Option

a. *This feature shall allow Guard Tour patrol sequences to be created consisting of a number of designated clocking points, which the patrolling guard has to visit.*

b. *A guard tour sequence shall define the order in which the clocking points are to be visited and also how long the guard should take to move between each clocking point location. A window of tolerance shall be included to add a +/- value to these timings.*

c. *The system operator shall initiate the required guard tour patrol and declares the guard who is to undertake the tour of the premises. The system shall then automatically monitor the guards progress around the patrol tour, reporting alarms if the clocking points are either out of sequence, or the guard arrives too early, or becomes overdue. The operator shall be notified as each point is clocked to allow the guard's progress around the site to be monitored. A patrol tour shall be able to be suspended, if required, and will automatically resume when the next point is then clocked.*

d. *Guard tour patrols shall be configurable on a per company basis when multiple companies are required on a site. Management reports shall be created from the history log to confirm when each guard tour was carried out, including any deviations or incidents during the tour.*

45. Thin Client Access Option

a. *The system shall provide for an option of thin client access to the Security Management System. The thin client interface shall utilize Citrix or Microsoft Remote Desktop Services or any other equivalent and compatible services to provide the same look and feel of the thick client to minimize training time and expense. The thin client shall be capable of the same functionality of a thick client with the exception of functionality that requires access to ports on the thin client computer – Microsoft Remote Desktop Services does not sufficiently support such access.*

b. *The system shall provide for an option of thin client access specifically for the visitor management system. The thin client interface shall utilize Citrix or Microsoft Remote Desktop Services to provide the same look and feel of the thick client to minimize training time and expense. The thin client shall be restricted to Visitor Management functions.*

46. Web Client Option

a. *The system shall provide a web browser interface to facilitate Security Management System operations using Windows Internet Information Services web server technology or any other equivalent and compatible techonology .*

b. *The Security Management System web client shall allow users to easily manage cardholders, visitors and alarms from any standard web browser.*

c. *Users shall be able to enter cardholder and visitor details, print and encode badges, sign visitors in and out, view card status, view the last 25 valid card transactions and manage alarms.*

d. *Language translations shall be available together with a documented process for adding further languages at a later date.*

e. *User interface language selection shall include the ability to manually override automatic system detection.*

f. *Language selection shall determine localized input field formats (dates for example dd/mm/yyyy, mm/dd/yy etc.)*

g. *There shall be no requirement to install additional software on the client machine hosting the web browser.*

47. Alarm Workflow Option

a. *The Security Management System shall provide the ability to create, find, view modify, copy or delete work flows.*

b. *A workflow shall be triggered automatically when a selected alarm or task based action is performed such as opening or acknowledging a new alarm or task.*

c. *When a trigger event occurs, the configured workflow action(s) shall be performed (for example, opening an Security Management System window, clearing a specified alarm type, displaying an instruction or sending an email)*

d. *Each workflow trigger shall allow more than one action to be performed.*

e. *Workflow actions shall allow question prompts and answer inputs. Answers shall be able to determine the path for further actions.*

f. *The order in which the actions are placed within each workflow shall determine the order in which they are executed.*

g. *Multiple Workflows shall be allowed for each trigger. The priority of multiple workflows for a single trigger shall be configurable.*

h. *Workflow Manager shall utilize a graphical flow chart design.*

i. *Workflow Manager shall be able to execute predefined commands.*

j. *Different workflows shall have the ability to automatically initiate for any device or any alarm type.*

k. *Workflows must have the ability to display alarm instructions.*

l. *Workflows shall have the ability to send automated emails or create tasks in the Task Manager.*

PROFESSIONAL SERVICES (PSG)

F. Manufacturer shall provide Professional Services for direct end user support through the awarded contractor.

1. All contractors shall provide Professional Services direct from the Manufacturer as follows:

a. *Bench Testing and Commissioning.*

b. *Custom reporting.*

c. *Human Resource Integrations.*

d. *Conversions.*

e. *Third party integrations.*

f. *Disaster recovery commissioning testing.*

G. Maintenance proposal should identify option for manufacturer provided Professional Services to include Life Cycle Management for ongoing system support

1. Optional elements for support should include:

a. *Program Management regularly scheduled calls to include manufacturer, integrator and end user.*

b. *Routine manufacturer audits and scheduled maintenance.*

c. *Manufacturer provided annual upgrade services.*

2. Bundled professional service options should be provided direct from the Manufacturer

WARRANTY

A. Contractor warrants that all Work furnished (material and labor) under this Contract will be of good quality, free from faults and defects, and in conformance with the Project Drawings and Specifications.

B. Contractor shall provide a parts and labor guarantee on all Work. Unless otherwise specified herein, Contractor's guarantee shall be for a period of one year from date of Acceptance, except where any specific guarantees from a supplier or equipment manufacturer extends for a longer time.

C. Contractor's guarantee shall cover all costs associated with troubleshooting, repair, and replacement of defective Work, including costs of labor, transportation, lodging, materials, and equipment.

SYSTEM STARTUP

A. Power shall only be applied to the system after re-checking for proper grounding of the system and measuring all loops for lack of shorts, grounds, and open circuits.

MAINTENANCE

A. Provide full procedures for all database back-ups.

B. Provide full procedures for server/workstation hard drive maintenance, such as defrag, etc.

C. Provide full procedures for maintaining physical and software firewalls.

D. Provide full procedures for upgrading software.

E. Provide full procedures for testing battery condition on all field panels for adequate back-up time.

F. Provide full procedures for any other tasks that must be performed to ensure the warranty remains intact.

PRODUCTS

GENERAL

A. All products not provided by the supplier shall be new and unused, and shall be of manufacturer's current and standard production.

B. Where two or more equipment items of the same kind are provided, all shall be identical and provided by the same manufacturer.

C. Drawings and Specifications indicate major system components, and may not show every component, connector, module, or accessory that may be required to support the operation specified. Contractor shall provide all components needed for complete and satisfactory operation.

D. Product Availability

1. Contractor, prior to submitting a proposal, shall determine product availability and delivery time, and shall include such considerations into his proposed Contract Time.
2. Certain products specified may only be available through factory authorized dealers and distributors. Contractor shall verify his ability to procure the products specified prior to submitting a proposal.

E. Wire and Cable

1. General: Provide all wire and cable required to install systems as indicated. Wire and cable shall be sized to provide minimum voltage drop and minimum resistance to the devices being supplied.
2. All cables shall be specifically designed for their intended use (direct burial, aerial, etc.).
3. Comply with equipment manufacturers recommendations for wire and cable size and type.
4. Comply with all applicable codes and ordinances.

WORKMANSHIP

A. Comply with highest industry standards, except when specified requirements indicate more rigid standards or more precise workmanship.

B. Perform Work with persons experienced and qualified to produce workmanship specified.

C. Maintain quality control over suppliers and Subcontractors.

D. Quality of workmanship is considered important. [CLIENT] Project Manager will have the authority to reject Work which does not conform to the Drawings and Specifications.

EQUIPMENT PRE-TEST

A. All equipment shall be bench tested prior to delivery to job site and prior to installation. Bench test per manufacturer's installation instructions.

TRAINING

A. Contractor shall provide complete operator training on the Security Management System. Training shall consist of thirty-two hours of classroom instruction for ten people selected by Owner, plus two (2) hours of individual hands-on training for each of ten people selected by Owner. Hands-on training shall include the opportunity for each person to operate the system, and to practice each operation that an operator would be expected to perform.

B. Training shall cover all operating features of the system, including the following:

1. System set-up and cardholder database configuration.
2. Access control features.
3. Alarm monitoring features.
4. Report generation and searches.
5. Card management and Badge Design/Printing
6. Disk backup procedures
7. Routine maintenance and adjustment procedures.

C. Training sessions are to be held at Owner's facility, and are to be scheduled at the convenience of Owner. Contractor shall provide written training outline and agenda for each training session prior to scheduling.

10. The qualified bidder should provide the algorithm for issuing of access cards to the Embassy. Accordingly, a non-disclosure agreement (as per **Annexure-6**) shall also be taken from the service provider to ensure the complete confidentiality of the algorithm used for programming of access cards. Further, there should be separate cabling for access control system.

11. Provision for battery back up should be to avoid any functionality issue during power failure.

--END OF SECTION--

SECTION IV : SUBMISSION OF PROPOSALS

Two bid system:

The two bid system will be followed for this tender. In this system, bidder must submit his officer in two separate sealed envelopes as explained below:

Envelope No. 1: "Technical Bid" shall contain:

Technical Bid should be prepared as per the instructions given in the Tender Documents along with all required information, documents in support of the minimum eligibility criteria, valid EMD of requisite amount. Documents comprising the Bid:

a. Technical Bid Submission Form (as per Annexure 5) duly signed and printed on Company's letterhead.

b. Contact Details Form, duly filled and signed & stamped**.**

c. Earnest Money Deposit of OMR 200.000 or a judicially valid Undertaking in lieu of EMD.

d. The bidder should submit an undertaking to the effect that a Performance Bank Guarantee (PBG) of 10% (Refer Section IV of the tender document) of the order value will be submitted in case the Embassy of India, Muscat decides to award the work to them.

e. Complete technical details and specifications alongwith brochure of the access control system (including details of controller, readers, etc.) proposed by the company

- The company shall enclose the full company profile (Annexure-5) with details of its registered office, the name & designation of its contact person along with his telephone/mobile no. and email address. The company should have a valid Registration No. and proof of the same is to be enclosed.

- The bidder should be a qualified and experienced company in providing / installing installation of security equipment for a minimum of 10 years. Details of similar nature of work done in other Embassies/Government offices/companies with proof should be attached.

- The company should have an established office with adequate number staff and infrastructure related to the concerned job in Muscat.

- No advance payment will be admissible. Payment will be made after successful and satisfactory completion of work.

- All necessary manpower, material and transport shall be the sole responsibility of the winning (L1) bidder.

- Duly filled in Technical Bid with proper seal and signature of authorized person on each page of the bid submitted.

Envelope 2: “Financial Bid” shall contain:

Price Schedule (duly filled in Annexure-1 and Annexure-2) complete in all respects with proper seal and signature of authorized person. Both the technical bid and financial bid envelopes should be sealed separately and clearly marked as “Envelope no. 1 - Technical Bid" and "Envelope no. 2 - Financial Bid". Both the sealed envelopes should be placed in a third larger envelope clearly mentioning “Technical Bid & Financial Bid” for “**Up-gradation of existing Access Control System installed in the Chancery of Embassy of India, Muscat**” and addressed to “Head of Chancery” Embassy of India, Muscat.

Note 1: Please write tender number on each envelope and seal all the envelopes.

Note 2: Please do not put "Financial Bid" (prices quoted) in the technical bid envelope. If the price quoted is submitted with technical bid, the tender will be rejected.

<u>Opening of Technical Bids:</u>

a. All the technical bids received by the Embassy of India, Muscat will be opened on **08th August, 2024 at 1500 hrs** in the Conference room of the Embassy of India, Muscat.

b. After being opened, the Technical Bids will be evaluated, by the Embassy ofIndia, Muscat, based on the available documents submitted by the bidder.

c. After evaluation of the Technical Bids, the Embassy of India, Muscat will intimate the date for opening of the Financial Bids of only those bidders who qualify at Technical Bid stage.

d. Financial Bids of those bidders who do not qualify at Technical Bid stage will be returned to the respective bidders un-opened.

<u>Opening of Financial bids :</u>

a. Financial bids of the short listed bidders only will be opened, in the presence of the bidders or their authorized representative, who choose to attend, date to be intimated later.

b. The authorized representative of bidders, present at the time of opening of the bids shall be required to sign an attendance sheet as a proof of having attended the financial bid opening.

c. The bidder‘s name, bid prices, discounts and such other details considered as appropriate by the Embassy of India, Muscat will be announced at the time of the opening of the bids.

d. Technically accepted competitive bids ONLY will be considered for the opening of Financial Bids.

Contact information
(Pardeep Kumar)
Head of Chancery
Embassy of India
Muscat
Tel. No. +968-2468 4566
Email: admin.muscat@mea.gov.in

SECTION V: PERFORMANCE BANK GUARANTEE (PBG)

Performance Security:

(a) The successful bidder has to deposit Performance Security which will be a sum equivalent to 10% of the accepted contract value in favour of ‘Embassy of India, Muscat’ payable at Muscat in the form of Demand draft/pay order/Bank Guarantee within 7 days of award of work, as per the format attached to this document (Refer Annexure–3) or in the form of security bond issued by recognised bank in Oman. This bank guarantee/bond shall remain valid till the completion of validity of contract.

(b) The PBG will be a sum equivalent to 10% of the accepted contract value in favour of ‘Embassy of India, Muscat ', payable at Muscat in form of Demand Draft / Pay Order/Bank Guarantee within seven days of the award of work. Performance Security should remain valid for a period of sixty (60) days after the successful completion of work. In case, the contract is further extended beyond the initial period, the PBG will have to be renewed accordingly by the bidder. No interest shall be paid on PBG.

(c) The Performance Security will be forfeited by order of the Competent Authority in Mission in the event of any breach or negligence or non-observance of any terms & conditions of the contract or for unsatisfactory performance or for non-acceptance of the work order. On expiry of the contract, portion of the Performance Security, as may deemed fit by the Mission sufficient to cover any incorrect or excess payments made on the bills to the firm, shall be retained until the final audit report on the account of Supplier's bill has been received and examined.

(d) If the Contractor fails to provide the Performance Security within seven days of the signing of agreement, such failure shall constitute a breach of the contract and the Mission shall be free to make other arrangements at the risk, cost and expense of the Contractor.

(e) On due performance and completion of the work in all respects, the Performance Security will be returned to the bidder without any interest on presentation of an absolute 'No Demand Certificate' from the bidder.

***

Annexure -1

Tender Submission Sheet

(To be submitted with the Financial bid only)

Invitation for Tender No: Date:

Tender Name:

To:

[Name and address of Employer]

We, the undersigned, offer to execute and complete in conformity with the Conditions of Contract and associated Contract Documents including Addenda Nos. ……. and maintain the whole of the said works at the rates quoted against each items in the Bill of Quantities.

The total price of our Tender is:
OMR: [insert value in figures]

[Insert value in Words]

Our Tender shall be valid for the period stated in the ITB and it shall remain binding upon us and may be accepted at any time before the expiration of that period. A Tender Security for an amount of OMR.________ only is attached in the form of a *[state pay order, bank draft]* valid for a period of 30 days beyond the contract period.

If our Tender is accepted, we commit to obtaining a Performance Security in the amount stated in the ITB and valid for a period of 30 days beyond the contract period.

We declare that the Government of Oman has not declared us, and any Subcontractors or Contractors for any part of the Contract ineligible on charges of engaging in corrupt, fraudulent, collusive or coercive practices.

We are not participating as Tenders in more than one Tender in this Tendering process. We understand that your written Notification of Award shall constitute the acceptance of our Tender and shall become a binding Contract between us, until a formal Contract is prepared and executed.

We understand that you are not bound to accept the lowest evaluated Tender or any other Tender that you may receive.

Signed
In the capacity of:
Duly authorised to sign the Tender on behalf of the Tender.

Annexure-2

FINANCIAL BID/PRICE SCHEDULE

Format for submission of financial bid for up-gradation of existing access control system installed in Embassy of India, Muscat (as per work schedule) to Embassy of India, Muscat

(To be submitted along with the financial bid only)

BID No. MUS/815/01/2021 Date: ……………………..

To,

Head of Chancery
Embassy of India,
Muscat, Oman

Price Schedule

S. No.	Work description	Total Bid Quantity	Total Price (in OMR)
1	**2**	**3**	**4**
1	Access Control Software	1	
2	Main Door Controller 4 readers with network connectivity	1	
3	Direct Controller 4 Readers	2	
4	Biometric Face Recognition Device + Card Reader (Supports HID prox) ***(as per required specifications, refer Section II of tender document)***	9	
5	**Lock** : 600Lbs,12VDC/24VDC SURFACE MOUNT MAGNETIC LOCK with Z / L Bracket ***(as per required specifications, refer Section II of tender document)***	8	
6	DOOR CONTACT SURFACE	8	
7	Touch less exit switch button	8	
8	Conduit and cable for the above system (LOT)	01	
9	Civil Work for the above (LOT)	01	
10	Server ***(as per required specifications, refer Section II of tender document)***	01	

11	POE switch ***(refer Section II of tender document)***	If required	
12	Termination, Testing, Commissioning of the Hardware and Software including training at local office for the above system	01	
13	Printing and supply of photo identity (RFID) cards with photo and other details provided by the Embassy	150	
		Taxes	
		Grand total	

Note: Above quoted price for up-gradation of existing access control system installed in Embassy of India, muscat (***as per scope of works and specifications mentioned Section – II of tender document***) is complete in all respect as per technical specifications and terms & conditions mentioned in the bid document.

Yours faithfully,

(Signature of Authorized Signatory)

Name:

Designation:

Company seal:

Annexure-3

PROFORMA OF BANK GUARANTEE

(on non-judicial paper of appropriate value)

To,

Head of Chancery
Embassy of India
Muscat, Oman

BANK GUARANTEE NO:

DATE:

Dear Sir(S)

This has reference to the Purchase Order No. ____________ Dated _________ been placed by Embassy of India to M/s (Name & Address of vendor) for.

The conditions of this order provide that the vendor shall,

1. Arrange to deliver the items listed in the said order to the consignee, as per details given in said order, and

2. Arrange for the comprehensive warranty service support towards the items supplied by vendor on site across Muscat, Oman, as per the warranty clause in said purchase order.

M/s …………………………………………….(Name of Vendor) has accepted the said purchase order with the terms and conditions stipulated therein and have agreed to issue the performance bank guarantee on their part, towards promises and assurance of their contractual obligations vide the purchase order No. _________________ M/s. ………………………………………………….. (name of vendor) holds a current account with us and has approached us and at their request and in consideration of the promises, we hereby furnish such guarantees as mentioned hereinafter.

Embassy of India, Muscat shall be at liberty without reference to the Bank and without affecting the full liability of the Bank hereunder to take any other undertaking of security in respect of the suppliers obligations and /or liabilities under or in connection with the said contract or to vary the terms vis-a-vis the supplier or the said contract or to grant time and or indulgence to the supplier or to reduce or to increase or otherwise vary the prices or the total contract value or to forebear from enforcement of all or any of the obligations of the supplier under the said contract and/or the remedies of the Embassy of India, Muscat under any security(ies) now, or hereafter held by the Embassy of India, Muscat and no such dealing(s) with the supplier or release or forbearance whatsoever shall have the effect of releasing the bank from its full liability of the Embassy of India, Muscat hereunder or of prejudicing right of the Embassy of India, Muscat against the bank.

This undertaking guarantee shall be a continuing undertaking guarantee and shall remain valid and irrevocable for all claims of the Embassy of India, Muscat and liabilities of the supplier arising upto and until date…….

Your right to recover the said sum of OMR.______________ (Omani Rial______________________ only) from us in manner aforesaid will not be affected/or suspended by reason of the fact that any dispute or disputes have been raised the said M/s and/or that any dispute or disputes are pending before any officer, tribunal or court or Arbitrator.

Our liability under this guarantee is restricted to OMR_____________ (Omani Rial ________________________________Only) Our guarantee shall remain in force until unless a suit action to enforce a claim under guarantee is filed against us within six months from (which is date of expiry of guarantee) all your rights under the said guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there under.

We have power to issue this guarantee in your favour under Memorandum and Articles of Association of our Bank and the undersigned has full power to do under the power of Attorney dated.

Notwithstanding anything contained herein:

A. Our liability under this guarantee shall not exceed OMR……………….(in words)

B. This bank guarantee shall be valid up to……& unless a suit for action to enforce a claim under guarantee is filed against us within six months from the date of expiry of guarantee. All your rights under the said guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there after i.e. after six months from the date of expiry of this Bank guarantee

C. We are liable to pay the guaranteed amount or any parts thereof under this bank guarantee only and only if you serve upon us a written claim or demand or before ………….

D. The Bank guarantee will expire on ………

Granted by the Bank

Yours faithfully,

For (Name of Bank)
SEAL OF THE BANK
Authorized Signatory

Annexure-4

(On the letterhead of the bidding company)

The Head of Chancery
Embassy of India, Muscat
Diplomatic Area, Al-Khuwair, Muscat, Oman

UNDERTAKING

I, ___________________, of M/s. ______________________________, having registered office at ______________________________________, do hereby undertake that my company,

M/s.___________________________, will not withdraw or modify its bids from Tender No. MUS/815/01/2021 dated 11.07.2024 for '**UP-GRADATION OF EXISTING ACCESS CONTROL SYSTEM INSTALLED IN EMBASSY OF INDIA, MUSCAT'** (as per work schedule mentioned in tender document)' at the Embassy of India, Muscat during the period of validity of the bids.

I further undertake to have understood that if my company M/s. _______________________ Enterprise withdraws or modifies its bids or if it fails to sign the contract or fails to submit a performance security before the stipulated deadline if the work is awarded to it, M/s. ___________________ will be suspended for a specified time period from being eligible to submit bids for contracts with Embassy of India, Muscat.

Place :
Date:

Annexure-5

Technical Bid Proforma

Format for submission of financial bid for up-gradation of existing access control system installed in Embassy of India, Muscat (as per work schedule) to Embassy of India, Muscat

Bidder's description format summary

Name of the Bidding Firm	
Name of Partner(s) & Nationality	
Name of the Authorized Signatory Nationality Passport No. E Mail ID Telephone No. Fax No.	
Year of Incorporation	
Registration No.	
Service tax no.	
Registered Office & Address	
Branch offices in (with address and Contact details) if any	
Average Annual turnover in the *last five* financial years	
Total Staff Strength *with Nationality of Employees*	
Total Technical staff percentage	
Nationality of Staff working in Company and to be deputed for work *(National of India or friendly country)*	
Details about key personnel of the bidding company (with id proof/supporting documents)	1. 2. 3. 4. 5.
Complete technical details/specifications and brochure of access control system (including controller, readers etc.) proposed by the company	

UNDERTAKING

a) I, the undersigned certify that I have gone through the terms and condition mentioned in the tender document and undertake to comply with them.
b) The rates quoted by me are valid and binding upon me for the entire period contract.
c) I hereby had undertaken to render the service as per direction given in the tender document.

Sign and stamp of authorized signatory of the company

Name:

Designation:

BIDDER INFORMATION (TO BE ATTACHED WITH TECHICAL BID)

(More detailed information on the following aspect may be given in typed form)

Business background	
How many years has your firm been in business? How many years under its present business name?	
Attach a current organizational chart and include the total number of employees in your firm in AAA, by various locations.	
Claims and Suits (Explain, if the answer is "Yes")	
Has your firm, its subsidiaries or its parent companies, ever filed for bankruptcy?	
Has your firm ever failed to complete work awarded to it?	
Are there any judgments, claims, arbitration proceedings or suits pending or outstanding against your firm or its officers?	
Has your firm filed any lawsuits or requested arbitration with regard to any contract(s) within the last five years?	
Financial Information	
Please provide copies of your firm's audited financial statements (income statement, balance sheet, cash flow statements) for the last 3 years.	
How long has your company been providing the services outlined in this Tender? Please list contact names and phone number for three (3) companies with which you have entered into facilities/property management contracts, and include a brief description of the scope covered under each.	
Please list your top five (5) customers and indicate what % of your business they represent.	
Who are your bankers?	

Sign and stamp of authorized signatory of the company

Name:
Designation:

Annexure - 6

NON-DISCLOSURE AGREEMENT

This Agreement is entered into this .....(Date) day of ....(Month), ...(Year) between .... (Name of the Mission) (hereinafter called as "**Discloser**") and ....(Name of the Company with Address) (hereinafter called as "**Recipient**"), collectively "**Party**" or "**Parties**".

WHEREAS the Discloser possesses certain information relating to the security set-up, security architecture, lay-out, security processes and procedures, designs, drawings, software and hardware configuration, computer programs, algorithms, services, customers etc that is confidential and proprietary in nature (hereinafter called as **"Confidential Information**"); and

WHEREAS the Recipient is bound to get to know about the Confidential Information in pursuant to the terms of the Agreement for the purpose of supply, installation, testing and commissioning of a Access Control System (hereinafter called as "**Purpose**") in the .... (**hereinafter called as "Premises"**);

NOW THEREFORE, in consideration for the mutual undertakings of the Discloser and the Recipient under this Agreement, the Parties agree as follows:

1. **Disclosure:** Recipient agrees not to disclose and the Discloser agrees to let the Recipient have the access to the Confidential Information as identified and reduced in writing or provided verbally or in any other way not reduced in writing at the time of such disclosure of the information.

2. **Confidentiality:**

2.1 No Use: Recipient agrees not to use the Confidential Information in any way or under any circumstances share the same, in writing or through any other means, with any Third Party.

2.2 No Unauthorized Disclosure: Recipient agrees to use its best efforts to prevent and protect the Confidential Information, or any part thereof, from disclosure *to any person(s) or entity(ies), even if authorized or directed under any law, without the express permission of the Discloser.* Discloser, notwithstanding, shall have the right to deny such disclosure of the Confidential Information being detrimental to the security interests of the Discloser and/or its premises and employees.

2.3 Protection of Secrecy: Recipient agrees to take all steps necessary to protect the secrecy of the Confidential Information, and to prevent the Confidential Information from falling into the public domain or into the possession of unauthorized person(s) and/or entity(ies).

2.4 Recipient agrees that the layout plan of the structural design of the Premises, whether in in physical or electronic form, shall always be in the custody of the Discloser. However, the Recipient shall have the access to the layout plan for the purpose of carrying out the contract for installation of Access Control System.

3. **Notices:** All notices hereunder shall be given by letter, addressed as follows:

[Name of the Mission/Post]
[Address]

Attention[Insert Name]
Title:[Insert Designation]
E-mail:[Insert E-mail]
Telephone:[Insert Number]
Fax:[Insert Number]

[Name of the Company]
[Address]

Attention:[Insert Name]
Title: [Insert Designation]
E-mail:[Insert E-mail]
Telephone:[Insert Number]
Fax:[Insert Number]

4. **Term and Termination.** The term of this Agreement shall commence on the Effective Date *i.e. the date of signing the Agreement for the Purpose* and continue for such a period *until and unless the Discloser terminates the Agreement or the Premises is relocated or vacated or abandoned, whichever is earlier.*

5. **Breach**. The Recipient acknowledges that disclosure or use of Confidential Information in violation of this Agreement could cause irreparable harm to Discloser *including loss of lives and limbs of the persons and damage to the property, for which monetary damages may be difficult to ascertain or turn to be meaningless.* The Recipient therefore agrees that Discloser will have the right, in addition to its other rights and remedies, to seek injunctive relief for violations of this Agreement.

6. In case the Discloser suspects any violation of this Agreement, upon reasonable notice, it shall be binding for the Recipient to allow the Discloser to carry out an Audit by itself or by an authorized representative. In such a situation, the Recipient shall cooperate with the Discloser. *The onus to rebut the suspicion shall lie on the Recipient.*

7. Any dispute or difference arising out of or in connection with this Non-Discloser Agreement shall be setteled amicably by the Parties through mutual negotiations. Any unsettled dispute or difference shall be referred to Arbitration by a Sole Arbitrator. The Arbitration shall be conducted in accordance with the rules and procedure of UNCITRAL in force on the date of Agreement. Arbitration proceedings shall be held in India and will be conducted in English. The decision of Arbitral Tribunal shall be final and binding on all Parties. Cost of Arbitrtaion shall be borne by Parties themselves unless and otherwise ordered by the Tribunal.

8. This Agreement shall be governed by and construed in accordance with the laws in force in India.

9. **Miscellaneous.**

   a) Except in the event of an amalgamation or merger with or take-over by a third party of their business, neither Party may assign or transfer its rights or obligations in this Agreement without the prior written consent of the other.

   b) The Parties do not intend that any agency or partnership relationship be created by them by this Agreement.

      19. All additions or modifications to this Agreement must be made in writing and signed by an authorized representative of each Party.

ACCEPTED AND AGREED

[Name of the Mission/Post]
[Address]

Attention:[Insert Name]
Title:[Insert Designation]
E-mail:[Insert E-mail]
Telephone:[Insert Number]
Fax:[Insert Number]

[Name of the Company]
[Address]

Attention:[Insert Name]
Title: [Insert Designation]
E-mail:[Insert E-mail]
Telephone:[Insert Number]
Fax:[Insert Number]