Amendment No. 5
to
Contract No. 5600 NS140000039
for
ESAS Maintenance & Support
between
Schneider Electric Buildings Americas, Inc. (Contractor)
and the
City of Austin

1.0 The Contract is hereby amended as follows:

The City exercises this amendment to extend the contract by 60 months, through July 31, 2023.

Exhibit A is amended as per the following attachment.

2.0 The total contract authorization is recapped below:

Action	Action Amount	Total Contract Amount
Initial Term: 08/01/2014 – 07/31/2015	$1,912,800.00	$1,912,800.00
Amendment No. 1: Option 1 – Extension 08/01/2015 – 07/31/2016	$1,442,500.00	$3,355,300.00
Amendment No. 2: Option 2 – Extension 08/01/2016 – 07/31/2017	$1,415,900.00	$4,771,200.00
Amendment No. 3: Change Request: reduce scope of work	(-$100,000.00)	$4,671,200.00
Amendment No. 4: Option 3 – Extension 08/01/2017 – 07/31/2018	$1,080,300.00	$5,751,500.00
Amendment No. 5: 60-month extension 08/01/2018 – 07/31/2023	$0.00	$5,751,500.00

3.0 MBE/WBE goals do not apply to this contract.

4.0 By signing this Amendment the Contractor certifies that the vendor and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the GSA List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

5.0 All other terms and conditions remain the same.

BY THE SIGNATURES affixed below, this amendment is hereby incorporated into and made a part of the above-referenced contract.

Sign/Date: 7/2/2018	Sign/Date:
Printed Name: Neal Eckles	Printed Name: JAMES T. HOWARD

Authorized Representative
Schneider Electric Buildings Americas, Inc.
1077 Central Parkway South, Suite 650
San Antonio, TX 78232

Authorized Representative
City of Austin
Purchasing Office
124 W. 8th Street, Ste. 310
Austin, Texas 78701

Pricing under this contract will be determined according to the National IPA pricing schedule. (http://www.nationalipa.org/Vendors/Pages/SchneiderElectric.aspx)

If any product or service is not found on National IPA pricing schedule, then pricing shall be no less than 10% off the MSRP for these products or services.

Amendment No. 4
to
Contract No. 5600 NS140000039
for
ESAS Maintenance & Support
between
Schneider Electric Buildings Americas, Inc. (Contractor)
and the
City of Austin

1.0 The City hereby exercises this extension option for the subject contract. This extension option will be August 01, 2017 through July 31, 2018. No options to extend remain.

2.0 The total contract amount is increased by $1,080,300.00 by this extension period. The total contract authorization is recapped below:

Action	Action Amount	Total Contract Amount
Initial Term: 08/01/2014 – 07/31/2015	$1,912,800.00	$1,912,800.00
Amendment No. 1: Option 1 – Extension 08/01/2015 – 07/31/2016	$1,442,500.00	$3,355,300.00
Amendment No. 2: Option 2 – Extension 08/01/2016 – 07/31/2017	$1,415,900.00	$4,771,200.00
Amendment No. 3: Change Request: reduce scope of work	(-$100,000.00)	$4,671,200.00
Amendment No. 4: Option 3 – Extension 08/01/2017 – 07/31/2018	$1,080,300.00	$5,751,500.00

3.0 MBE/WBE goals do not apply to this contract.

4.0 By signing this Amendment the Contractor certifies that the vendor and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the GSA List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

5.0 All other terms and conditions remain the same.

BY THE SIGNATURES affixed below, this amendment is hereby incorporated into and made a part of the above-referenced contract.

Sign/Date: 06/11/2017

Printed Name: Neal Eckles-District General Manager
Authorized Representative

Schneider Electric Buildings Americas, Inc.
1077 Central Parkway South, Suite 650
San Antonio, TX 78232

Sign/Date:

Printed Name: JAMES T. HOWARD

Authorized Representative
City of Austin
Purchasing Office
124 W. 8th Street, Ste. 310
Austin, Texas 78701

Amendment No. 3
to
Contract No. NS140000039
for
ESAS Maintenance & Support
between
Schneider Electric Buildings Americas, Inc. (Contractor)
and the
City of Austin

1.0 The above referenced contract is amended as follows:

Revise the **Compensation** Section to **decrease the total not to exceed to** $4,671,200.00. This is a decrease of $100,000.00; and

2.0 The total Contract authorization is recapped below:

Term	Action Amount	Total Contract Amount
Initial Term: 08/01/2014 – 07/31/2015	$1,912,800.00	$1,912,800.00
Amendment No. 1: Option 1 - Extension 08/01/2015 – 07/31/2016	$1,442,500.00	$3,355,300.00
Amendment No. 2: Option 2 - Extension 08/01/2016 – 07/31/2017	$1,415,900.00	$4,771,200.00
Amendment No. 3: Change Request: reduce scope of work	(-$100,000.00)	$4,671,200.00

3.0 MBE/WBE goals were not established for this contract.

4.0 By signing this amendment the Contractor certifies that the Contractor and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the General Services Administration (GSA) List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas or the City of Austin.

5.0 All other terms and conditions remain the same.

By the signature affixed below, this amendment is hereby incorporated into and made a part of the above referenced contract.

Authorized Representative:

Contractor Signature:

Printed Name: NEAL J. ECKLES

Date: 10/17/2016

Schneider Electric Buildings Americas, Inc.
1077 Central Parkway South, Suite 650
San Antonio, Texas 78232

Signature:
City of Austin Purchasing Office
Printed Name: JAMES T. HOWARD

Date: 11/2/16

City of Austin
124 W. 8th St., Ste. 310
Austin, TX 78701

Amendment No. 2
to
Contract No. NS140000039
for
ESAS Maintenance & Support
between
Schneider Electric Buildings Americas, Inc.
and the
City of Austin

1.0 The City hereby exercises this extension option for the subject contract. This extension option will be effective August 01, 2016 to July 31, 2017. One option will remain.

2.0 The total contract amount is increased by $1,415,900 by this extension period. The total contract authorization is recapped below:

Action	Action Amount	Total Contract Amount
Initial Term: 08/01/2014 – 07/31/2015	$1,912,800.00	$1,912,800.00
Amendment No. 1: Option 1 – Extension 08/01/2015 – 07/31/2016	$1,442,500.00	$3,355,300.00
Amendment No. 2: Option 2 – Extension 08/01/2016 – 07/31/2017	$1,415,900.00	$4,771,200.00

3.0 MBE/WBE goals do not apply to this contract.

4.0 By signing this Amendment the Contractor certifies that the vendor and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the GSA List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

5.0 All other terms and conditions remain the same.

BY THE SIGNATURES affixed below, this amendment is hereby incorporated into and made a part of the above-referenced contract.

Sign/Date: Greg Jones 7/29/2016

Printed Name: Gregory Jones
Authorized Representative

Gregory Jones
Schneider Electric Buildings Americas, Inc.
1077 Central Parkway South, Suite 650
San Antonio, Texas 78232
Greg.s.jones@schneider-electric.com
210-483-5361

Sign/Date: Shawn Willett 8/9/16

Shawn Willett
Deputy Purchasing Officer

City of Austin
Purchasing Office
124 W. 8th Street, Ste. 310
Austin, Texas 78701

jb

Amendment No. 1
of
Contract No. NS140000039
for
Electronic Safety and Security Systems Maintenance and Support
between
Schneider Electric Buildings Americas, Inc. dba
Schneider Electric
and the
City of Austin

1.0 The City hereby exercises the extension option for the above-referenced contract. Effective August 1, 2015, the term for the extension option will be August 1, 2015 to July 31, 2016 and there are two remaining options.

2.0 The total contract amount is increased by $1,442,500.00 for the extension option period. The total Contract authorization is recapped below:

Term	Action Amount	Total Contract Amount
Basic Term: 08/01/14 – 07/31/15	$1,912,800.00	$1,912,800.00
Amendment No. 2: Option 1 08/01/15 – 07/31/16	$1,442,500.00	$3,355,300.00

3.0 MBE/WBE goals were not established for this contract.

4.0 By signing this Amendment the Contractor certifies that the Contractor and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the General Services Administration (GSA) List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

5.0 All other terms and conditions remain the same.

BY THE SIGNATURES affixed below, this Amendment is hereby incorporated into and made a part of the above-referenced contract.

Signature & Date: 8/19/15
Printed Name: JOHN C COLLINS
Authorized Representative VP South Region

Schneider Electric Buildings Americas, Inc.
Dba Schneider Electric
9101 Burnet Road Ste. 202
Austin, TX 78758-45132

Signature & Date: Shawn Willett
Shawn Willett, Corporate Contract Compliance Manager,
IT Procurement
City of Austin
Purchasing Office

CONTRACT BETWEEN THE CITY OF AUSTIN
AND
Schneider Electric Buildings Americas, Inc.
For
Electronic Safety and Security Systems Maintenance and Support

This Contract is made by and between the City of Austin ("City"), a home-rule municipality incorporated by the State of Texas, and Schneider Electric Buildings Americas, Inc. ("Contractor"), having offices at 1077 Central Parkway South, Suite 200, San Antonio, TX 78232.

SECTION 1. GRANT OF AUTHORITY, SERVICES AND DUTIES

1.1 **Engagement of the Contractor.** Subject to the general supervision and control of the City and subject to the provisions of the Terms and Conditions contained herein, the Contractor is engaged to provide the services set forth in Section 2, Scope of Work.

1.2 **Responsibilities of the Contractor.** The Contractor shall provide all technical and professional expertise, knowledge, management, and other resources required for accomplishing all aspects of the tasks and associated activities identified in the Scope of Work. In the event that the need arises for the Contractor to perform services beyond those stated in the Scope of Work, the Contractor and the City shall negotiate mutually agreeable terms and compensation for completing the additional services.

1.3 **Responsibilities of the City.** The City's Contract Manager will be responsible for exercising general oversight of the Contractor's activities in completing the Scope of Work. Specifically, the Contract Manager will represent the City's interests in resolving day-to-day issues that may arise during the term of this Contract, shall participate regularly in conference calls or meetings for status reporting, shall promptly review any written reports submitted by the Contractor, and shall approve all invoices for payment, as appropriate. The City's Contract Manager shall give the Contractor timely feedback on the acceptability of progress and task reports.

1.4 **Designation of Key Personnel.** The Contractor's Contract Manager for this engagement shall be Gregory Jones, Phone: (210) 483-5361, Email Address: Greg.S.Jones@Schneider-electric.com. The City's Contract Manager for the engagement shall be Walker Guthrie, Phone: (512) 974-1679, Email Address: Walker.Guthrie@austintexas.gov. The City and the Contractor resolve to keep the same key personnel assigned to this engagement throughout its term. In the event that it becomes necessary for the Contractor to replace any key personnel, the replacement will be an individual having equivalent experience and competence in executing projects such as the one described herein. Additionally, the Contractor will promptly notify the City Contract Manager and obtain approval for the replacement. Such approval shall not be unreasonably withheld.

SECTION 2. SCOPE OF WORK

2.1 **Contractor's Obligations.** The Contractor shall fully and timely provide all Deliverables described in the Solicitation and in the Contractor's Offer in strict accordance with the terms, covenants, and conditions of the Contract and all applicable Federal, State, and local laws, rules, and regulations.

SECTION 3. COMPENSATION

3.1 **Contract Amount.** The Contractor will be paid as indicated herein upon the successful completion of the Scope of Work. In consideration for the services to be performed under this Contract, the Contractor shall be paid an amount not to exceed $1,912,800.00 with three 12-month extension options in amounts not to exceed $1,442,500.00 for the first extension option, $1,415,900.00 for the second option, and $1,080,300.00 for the third extension option, for a total contract amount not to exceed $5,851,500.00.

3.2 **Economic Price Adjustment**.

3.2.1 **Price Adjustments.** Prices shown in this Contract shall remain firm for the first 12-month period of the Contract. After that, in recognition of the potential for fluctuation of the Contractor's cost, a price adjustment (increase or decrease) may be requested by either the City or the Contractor on the anniversary date of the Contract or as may otherwise be specified herein. The percentage change between the contract price and the requested price shall not exceed the percentage change between the specified index in effect on the date the solicitation closed and the most recent, non-preliminary data at the time the price adjustment is requested. The requested price adjustment shall not exceed ten percent (10%) for any single line item and in no event shall the total amount of the contract be automatically adjusted as a result of the change in one or more line items made pursuant to this provision. Prices for products or services unaffected by verifiable cost trends shall not be subject to adjustment.

3.2.2 **Effective Date.** Approved price adjustments will go into effect on the first day of the upcoming renewal period or anniversary date of contract award and remain in effect until contract expiration unless changed by subsequent amendment.

3.2.3 **Adjustments.** A request for price adjustment must be made in writing and submitted to the other Party prior to the yearly anniversary date of the Contract; adjustments may only be considered at that time unless otherwise specified herein. Requested adjustments must be solely for the purpose of accommodating changes in the Contractor's direct costs. Contractor shall provide an updated price listing once agreed to adjustment(s) have been approved by the parties.

3.2.4 **Indexes.** In most cases an index from the Bureau of Labor Standards (BLS) will be utilized; however, if there is more appropriate, industry recognized standard then that index may be selected.

3.2.4.1 The following definitions apply:

3.2.4.1.1 **Base Period:** Month and year of the original contracted price (the solicitation close date).

3.2.4.1.2 **Base Price:** Initial price quoted, proposed and/or contracted per unit of measure.

3.2.4.1.3 **Adjusted Price:** Base Price after it has been adjusted in accordance with the applicable index change and instructions provided.

3.2.4.1.4 **Change Factor:** The multiplier utilized to adjust the Base Price to the Adjusted Price.

3.2.4.1.5 **Weight %:** The percent of the Base Price subject to adjustment based on the index change.

3.2.4.2 **Adjustment-Request Review.** Each adjustment-request received will be reviewed and compared to changes in the index(es) identified below. Where applicable:

3.2.4.2.1 Utilize final Compilation data instead of Preliminary data

3.2.4.2.2. If the referenced index is no longer available shift up to the next higher category index.

3.2.4.3 **Index Identification.** Complete table as they may apply.

Weight % or $ of Base Price: 100	
Database Name: Producer Price Index Industry Data	
Series ID: PCU523---523---	
☒ Not Seasonally Adjusted	☐ Seasonally Adjusted

Geographical Area: Security Commodity Contract and Like Activity
Description of Series ID: Security Commodity Contract and Like Activity
This Index shall apply to the following items of the Bid Sheet / Cost Proposal: ALL

3.2.5 **Calculation.** Price adjustment will be calculated as follows:

3.2.5.1 **Single Index.** Adjust the Base Price by the same factor calculated for the index change.

Index at time of calculation
Divided by index on solicitation close date
Equals Change Factor
Multiplied by the Base Price
Equals the Adjusted Price

3.2.6 If the requested adjustment is not supported by the referenced index, the City, as its sole discretion, may consider approving an adjustment on fully documented market increases.

3.3 **Invoices.**

3.3.1 The Contractor shall submit separate invoices in duplicate on each purchase order or purchase release after each delivery. If partial shipments or deliveries are authorized by the City, a separate invoice must be sent for each shipment or delivery made.

3.3.2 **Proper Invoices must include a unique invoice number, the purchase order or delivery order number and the master agreement number if applicable, the Department's Name, and the name of the point of contact for the Department**. Invoices shall be itemized and transportation charges, if any, shall be listed separately. A copy of the bill of lading and the freight waybill, when applicable, shall be attached to the invoice. The Contractor's name and, if applicable, the tax identification number on the invoice must exactly match the information in the Vendor's registration with the City. Unless otherwise instructed in writing, the City may rely on the remittance address specified on the Contractor's invoice.

3.3.3 Invoices for labor shall include a copy of all time-sheets with trade labor rate and Deliverables order number clearly identified. Invoices shall also include a tabulation of work-hours at the appropriate rates and grouped by work order number. Time billed for labor shall be limited to hours actually worked at the work site.

3.3.4 Unless otherwise expressly authorized in the Contract, the Contractor shall pass through all Subcontract and other authorized expenses at actual cost without markup.

3.3.5 Federal excise taxes, State taxes, or City sales taxes must not be included in the invoiced amount. The City will furnish a tax exemption certificate upon request.

3.4 **Payment.**

3.4.1 All proper invoices received by the City will be paid within thirty (30) calendar days of the City's receipt of the Deliverables or of the invoice, whichever is later.

3.4.2 **If payment is not timely made, (per paragraph A), interest shall accrue on the unpaid balance at the lesser of the rate specified in Texas Government Code Section 2251.025 or the maximum lawful rate; except, if payment is not timely made for a reason for which the City may withhold payment hereunder, interest shall not accrue until ten (10) calendar days after the grounds for withholding payment have been resolved.**

3.4.3 If partial shipments or deliveries are authorized by the City, the Contractor will be paid for the partial shipment or delivery, as stated above, provided that the invoice matches the shipment or delivery.

3.4.4 The City may withhold or set off the entire payment or part of any payment otherwise due the Contractor to such extent as may be necessary on account of:

3.4.4.1 delivery of defective or non-conforming Deliverables by the Contractor;

3.4.4.2 third party claims, which are not covered by the insurance which the Contractor is required to provide, are filed or reasonable evidence indicating probable filing of such claims;

3.4.4.3 failure of the Contractor to pay Subcontractors, or for labor, materials or equipment;

3.4.4.4 damage to the property of the City or the City's agents, employees or contractors, which is not covered by insurance required to be provided by the Contractor;

3.4.4.5 reasonable evidence that the Contractor's obligations will not be completed within the time specified in the Contract, and that the unpaid balance would not be adequate to cover actual or liquidated damages for the anticipated delay;

3.4.4.6 failure of the Contractor to submit proper invoices with all required attachments and supporting documentation; or

3.4.4.7 failure of the Contractor to comply with any material provision of the Contract Documents.

3.4.5 Notice is hereby given of Article VIII, Section 1 of the Austin City Charter which prohibits the payment of any money to any person, firm or corporation who is in arrears to the City for taxes, and of §2-8-3 of the Austin City Code concerning the right of the City to offset indebtedness owed the City.

3.4.6 Payment will be made bycheck unless the parties mutually agree to payment by credit card or electronic transfer of funds. The Contractor agrees that there shall be no additional charges, surcharges, or penalties to the City for payments made by credit card or electronic funds transfer.

3.4.7 The awarding or continuation of this contract is dependent upon the availability of funding. The City's payment obligations are payable only and solely from funds Appropriated and available for this contract. The absence of Appropriated or other lawfully available funds shall render the Contract null and void to the extent funds are not Appropriated or available and any Deliverables delivered but unpaid shall be returned to the Contractor. The City shall provide the Contractor written notice of the failure of the City to make an adequate Appropriation for any fiscal year to pay the amounts due under the Contract, or the reduction of any Appropriation to an amount insufficient to permit the City to pay its obligations under the Contract. In the event of non or inadequate appropriation of funds, there will be no penalty nor removal fees charged to the City.

3.5 PERFORMANCE BOND:

3.5.1 The Contractor may be required to provide a Performance Bond for an individual project in an amount equal to 100% of the cost of the project as specified in the Contract. The Performance Bond serves as security for the faithful performance of all of the Contractor's obligations under the Contract. The Performance Bond shall be issued by a solvent company authorized to do business in the State of Texas, and shall meet any other requirements established by law or by the City pursuant to applicable law. The Surety must obtain reinsurance for any portion of the risk that exceeds 10% of the Surety's capital and surplus. For bonds exceeding $100,000, the Surety must also hold a certificate of authority from the U.S. Secretary of the Treasury or have obtained reinsurance from a reinsurer that is authorized as a reinsurer in Texas and holds a certificate of authority from the U.S. Secretary of the Treasury.

3.5.2 The Performance Bond shall remain in effect throughout the term of the project.

3.6 **TRAVEL EXPENSES**: All travel, lodging and per diem expenses in connection with the Contract for which reimbursement may be claimed by the Contractor under the terms of the Solicitation will be reviewed against the City's Travel Policy as published and maintained by the City's Controller's Office and the Current United States General Services Administration Domestic Per Diem Rates (the "Rates") as published and maintained on the Internet at:

`http://www.gsa.gov/portal/category/21287`

No amounts in excess of the Travel Policy or Rates shall be paid. All invoices must be accompanied by copies of detailed itemized receipts (e.g. hotel bills, airline tickets). No reimbursement will be made for expenses not actually incurred. Airline fares in excess of coach or economy will not be reimbursed. Mileage charges may not exceed the amount permitted as a deduction in any year under the Internal Revenue Code or Regulations.

3.7 **FINAL PAYMENT AND CLOSE-OUT**:

3.7.1 If an MBE/WBE Program Compliance Plan is required by the Solicitation, and the Contractor has identified Subcontractors, the Contractor is required to submit a Contract Close-Out MBE/WBE Compliance Report to the Project manager or Contract manager no later than the 15th calendar day after completion of all work under the contract. Final payment, retainage, or both may be withheld if the Contractor is not in compliance with the requirements of the Compliance Plan as accepted by the City.

3.7.2 The making and acceptance of final payment will constitute:

3.7.2.1 a waiver of all claims by the City against the Contractor, except claims (1) which have been previously asserted in writing and not yet settled, (2) arising from defective work appearing after final inspection, (3) arising from failure of the Contractor to comply with the Contract or the terms of any warranty specified herein, (4) arising from the Contractor's continuing obligations under the Contract, including but not limited to indemnity and warranty obligations, or (5) arising under the City's right to audit; and

3.7.2.2 a waiver of all claims by the Contractor against the City other than those previously asserted in writing and not yet settled.

SECTION 4. TERM AND TERMINATION

4.1 **Term of Contract.** The Contract shall be in effect for an initial term of 12 months and may be extended thereafter for up to 3 additional 12 month periods, subject to the approval of the Contractor and the City Purchasing Officer or his designee.

4.1.1 Upon expiration of the initial term or period of extension, the Contractor agrees to hold over under the terms and conditions of this Contract for such a period of time as is reasonably necessary to re-solicit and/or complete the project (not to exceed 120 calendar days unless mutually agreed on in writing).

4.2 **Right To Assurance.** Whenever one party to the Contract in good faith has reason to question the other party's intent to perform, demand may be made to the other party for written assurance of the intent to perform. In the event that no assurance is given within the time specified after demand is made, the demanding party may treat this failure as an anticipatory repudiation of the Contract.

4.3 **Default.** The Contractor shall be in default under the Contract if the Contractor (a) fails to fully, timely and faithfully perform any of its material obligations under the Contract, (b) fails to provide adequate assurance of performance under Paragraph 24, (c) becomes insolvent or seeks relief under the bankruptcy laws of the United States or (d) makes a material misrepresentation in Contractor's Offer, or in any report or deliverable required to be submitted by the Contractor to the City.

4.4 **Termination For Cause.**. In the event of a default by the Contractor, the City shall have the right to terminate the Contract for cause, by written notice effective ten (10) calendar days, unless otherwise specified, after the date of such notice, unless the Contractor, within such ten (10) day period, cures such default, or provides evidence sufficient to prove to the City's reasonable satisfaction that such default does not, in fact, exist. The City may place Contractor on probation for a specified period of time within which the Contractor must correct any non-compliance issues. Probation shall not normally be for a period of more than nine (9) months, however, it may be for a longer period, not to exceed one (1) year depending on the circumstances. If the City determines the Contractor has failed to perform satisfactorily during the probation period, the City may proceed with suspension. In the event of a default by the Contractor, the City may suspend or debar the Contractor in accordance with the "City of Austin Purchasing Office Probation, Suspension and Debarment Rules for Vendors" and remove the Contractor from the City's vendor list for up to five (5) years and any Offer submitted by the Contractor may be disqualified for up to five (5) years. In addition to any other remedy available under law or in equity, the City shall be entitled to recover all actual damages, costs, losses and expenses, incurred by the City as a result of the Contractor's default, including, without limitation, cost of cover, reasonable attorneys' fees, court costs, and prejudgment and post-judgment interest at the maximum lawful rate. All rights and remedies under the Contract are cumulative and are not exclusive of any other right or remedy provided by law.

4.5 **Termination Without Cause.** The City shall have the right to terminate the Contract, in whole or in part, without cause any time upon thirty (30) calendar days' prior written notice. Upon receipt of a notice of termination, the Contractor shall promptly cease all further work pursuant to the Contract, with such exceptions, if any, specified in the notice of termination. The City shall pay the Contractor, to the extent of funds Appropriated or otherwise legally available for such purposes, for all goods delivered and services performed and obligations incurred prior to the date of termination in accordance with the terms hereof.

4.6 **Fraud.** Fraudulent statements by the Contractor on any Offer or in any report or deliverable required to be submitted by the Contractor to the City shall be grounds for the termination of the Contract for cause by the City and may result in legal action.

SECTION 5. OTHER DELIVERABLES

5.1 **Insurance**: The following insurance requirements apply.

5.1.1 **General Requirements.**

5.1.1.1 The Contractor shall at a minimum carry insurance in the types and amounts indicated herein for the duration of the Contract and during any warranty period.

5.1.1.2 The Contractor shall provide a Certificate of Insurance as verification of coverages required below to the City at the below address prior to contract execution and within 14 calendar days after written request from the City. Failure to provide the required Certificate of Insurance may subject the Offer to disqualification from consideration for award.

5.1.1.3 The Contractor shall not commence work until the required insurance is obtained and until such insurance has been reviewed by the City. Approval of insurance by the City shall not relieve or decrease the liability of the Contractor hereunder and shall not be construed to be a limitation of liability on the part of the Contractor.

5.1.1.4 The City may request that the Contractor submit certificates of insurance to the City for all subcontractors prior to the subcontractors commencing work on the project.

5.1.1.5 The Contractor's and all subcontractors' insurance coverage shall be written by companies licensed to do business in the State of Texas at the time the policies are issued and shall be written by companies with A.M. Best ratings of B+VII or better.

5.1.1.6 The Certificate of Insurance, and updates, shall be mailed to the following address:

City of Austin
Purchasing Office
P. O. Box 1088
Austin, Texas 78767

5.1.1.7 The "other" insurance clause shall not apply to the City where the City is an additional insured shown on any policy. It is intended that policies required in the Contract, covering -the Contractor with the City as an additional insured, shall be considered primary coverage as applicable.

5.1.1.8 If insurance policies are not written for amounts specified in Section 0400, Supplemental Purchase Provisions, the Contractor shall carry Umbrella or Excess Liability Insurance for any differences in amounts specified. If Excess Liability Insurance is provided, it shall follow the form of the primary coverage.

5.1.1.9 In the event of a claim, and if requested by the City, Contractor shall provide policy information upon request as needed to settle such claim.

5.1.1.10 The City reserves the right to review the insurance requirements set forth during the effective period of the Contract and to make reasonable adjustments to insurance requirements under this Contract with regard to insurance limits when deemed necessary and prudent by the City based upon changes in statutory law, court decisions, the claims history of the industry or financial condition of the insurance company as well as the Contractor.

5.1.1.11 The Contractor shall not cause any insurance to be canceled nor permit any insurance to lapse during the term of the Contract or as required in the Contract.

5.1.1.12 The Contractor shall be responsible for premiums, deductibles and self-insured retentions, if any, stated in policies. Self-insured retentions shall be disclosed on the Certificate of Insurance.

5.1.1.13 The Contractor shall endeavor to provide the City thirty (30) calendar days' written notice of erosion of the aggregate limits below occurrence limits for all applicable coverages indicated within the Contract.

5.1.1.14 The insurance coverages are required minimums and are not intended to limit the responsibility or liability of the Contractor.

5.1.2 **Specific Coverage Requirements.** The Contractor shall at a minimum carry insurance in the types and amounts indicated below for the duration of the Contract, including extension options and hold over periods, and during any warranty period. These insurance coverages are required minimums and are not intended to limit the responsibility or liability of the Contractor.

5.1.2.1 **Commercial General Liability Insurance.** The minimum bodily injury and property damage per occurrence are $500,000 for coverages A (Bodily Injury and Property Damage) and B (Personal and Advertising Injury).

5.1.2.1.1 Contractual liability coverage for liability assumed under the Contract and all other Contracts related to the project.

5.1.2.1.2 Contractor/Subcontracted Work.

5.1.2.1.3 Products/Completed Operations Liability for the duration of the warranty period.

5.1.2.1.4 Waiver of Subrogation, Endorsement CG 2404, or equivalent coverage.

5.1.2.1.5 Thirty (30) calendar days Notice of Cancellation, Endorsement CG 0205, or equivalent coverage.

5.1.2.1.6 The City of Austin listed as an additional insured, Endorsement CG 2010, or equivalent coverage.

5.1.2.2 **Business Automobile Liability Insurance.** The Contractor shall provide coverage for all owned, non-owned and hired vehicles with a minimum combined single limit of $500,000 per occurrence for bodily injury and property damage. Alternate acceptable limits are $250,000 bodily injury per person, $500,000 bodily injury per occurrence and at least $100,000 property damage liability per accident. The policy shall contain the following endorsements:

5.1.2.2.1 Waiver of Subrogation, Endorsement CA0444, or equivalent coverage.

5.1.2.2.2 Thirty (30) calendar days Notice of Cancellation, Endorsement CA0244, or equivalent coverage.

5.1.2.2.3 The City of Austin listed as an additional insured, Endorsement CA2048, or equivalent coverage.

5.1.2.3 **Worker's Compensation and Employers' Liability Insurance**. Coverage shall be consistent with statutory benefits outlined in the Texas Worker's Compensation Act (Section 401). The minimum policy limits for Employer's Liability are $100,000 bodily injury each accident, $500,000 bodily injury by disease policy limit and $100,000 bodily injury by disease each employee. The policy shall contain the following provisions and endorsements:

5.1.2.3.1 The Contractor's policy shall apply to the State of Texas.

5.1.2.3.2 Waiver of Subrogation, Form WC420304, or equivalent coverage.

5.1.2.3.3 Thirty (30) calendar days Notice of Cancellation, Form WC420601, or equivalent coverage.

5.1.2 **Endorsements.** The specific insurance coverage endorsements specified above, or their equivalents must be provided. In the event that endorsements, which are the equivalent of the required coverage, are proposed to be substituted for the required coverage, copies of the equivalent endorsements must be provided for the City's review and approval.

5.1.3 **Notice of Cancellation**: Notwithstanding any provision to the contrary in this Agreement, should any of the described policies be cancelled before the expiration date thereof, notice will be delivered in accordance with the policy provisions (pursuant to ISO ACORD Form 25 (2010/05)). In the event of such cancellation, and within ten (10) days of Contractor's receipt of such notification, Contractor will provide the City written notice of the cancellation or non-renewal (without replacement) of any policy of insurance referred to herein, and Contractor agrees to indemnify the City for any loss suffered by the City to the extent that such loss is attributable solely to Contractor's failure to provide such notice.

5.2 **Equal Opportunity.**

5.2.1 **Equal Employment Opportunity.** No Offeror, or Offeror's agent, shall engage in any discriminatory employment practice as defined in Chapter 5-4 of the City Code. No Offer submitted to the City shall be considered, nor any Purchase Order issued, or any Contract awarded by the City unless the Offeror has executed and filed with the City Purchasing Office a current Non-Discrimination Certification. Non-compliance with Chapter 5-4 of the City Code may result in sanctions, including termination of the contract and the Contractor's suspension or debarment from participation on future City contracts until deemed compliant with Chapter 5-4.

5.2.2 **Americans With Disabilities Act (ADA) Compliance.** No Offeror, or Offeror's agent, shall engage in any discriminatory employment practice against individuals with disabilities as defined in the ADA.

5.3 **Acceptance of Incomplete or Non-Conforming Deliverables.** If, instead of requiring immediate correction or removal and replacement of defective or non-conforming Deliverables, the City prefers to accept it, the City may do so. The Contractor shall pay all claims, costs, losses and damages attributable to the City's evaluation of and determination to accept such defective or non-conforming Deliverables. If any such acceptance occurs prior to final payment, the City may deduct such amounts as are necessary to compensate the City for the diminished value of the defective or non-conforming Deliverables. If the acceptance occurs after final payment, such amount will be refunded to the City by the Contractor.

5.4 **Delays.**

5.4.1 The City may delay scheduled delivery or other due dates by written notice to the Contractor if the City deems it is in its best interest. If such delay causes an increase in the cost of the work under the Contract, the City and the Contractor shall negotiate an equitable adjustment for costs incurred by the Contractor in the Contract price and execute an amendment to the Contract. The Contractor must assert its right to an adjustment within thirty (30) calendar days from the date of receipt of the notice of delay. Failure to agree on any adjusted price shall be handled under the Dispute Resolution process specified in paragraph 49. However, nothing in this provision shall excuse the Contractor from delaying the delivery as notified.

5.4.2 Neither party shall be liable for any default or delay in the performance of its obligations under this Contract if, while and to the extent such default or delay is caused by acts of God, fire, riots, civil commotion, labor disruptions, sabotage, sovereign conduct, or any other cause beyond the reasonable control of such Party. In the event of default or delay in contract performance due to any of the foregoing causes, then the time for completion of the services will be extended; provided, however, in such an event, a conference will be held within three (3) business days to establish a mutually agreeable period of time reasonably necessary to overcome the effect of such failure to perform.

5.5 **Ownership And Use Of Deliverables.** The City and Contractor do not envision the transfer of any patents, trademarks, copyrights, inventions, developments, improvements, ideas, trade secrets, or the like ("Intellectual Property") in connection with the Services to be provided under this Contract. Should the parties choose to pursue such activities, they shall enter into an appropriate separate written agreement concerning the development and ownership of such inventions and/or Intellectual Property. However, to the extent that a Deliverable or Service is or contains Intellectual Property that is; (i) conceived, discovered, invented, created, developed and/or reduced to practice exclusively by the City; (ii) created in connection with the Contractor's work for the City pursuant to this Contract and will only work exclusively with the proprietary system of the City (which shall be considered a "work made for hire"); or (iii) under a specific agreement for the joint development of Intellectual Property, such Intellectual Property will be owned exclusively by the City. Except for such Intellectual Property owned by the City as provided above, City acknowledges that Contractor is the exclusive owner of all right, title and interest in and any other deliverables produced and or provided under this Agreement, including, without limitation, its intellectual property, including patents, trademarks, trade secrets, and copyrights, methodologies and methods of analysis, ideas, concepts, expressions, know how, methods, techniques, skills, knowledge and experience (collectively, the "Contractor Intellectual Property") possessed by Contractor prior to, or acquired by Contractor during, the performance of this Contract and the same shall not be deemed to be "work made for hire" and Contractor shall not be restricted in any way with respect thereto. Contractor grants to the City a perpetual, paid-up, non-exclusive, royalty-free, worldwide license to make use of Contractor's Intellectual Property, including software that relate in any way to the operation, maintenance and improvement of any Deliverable or Service.

5.6 **Rights to Proposal and Contractual Material.** All material submitted by the Contractor to the City shall become property of the City upon receipt. Any portions of such material claimed by the Contractor to be proprietary must be clearly marked as such. Determination of the public nature of the material is subject to the Texas Public Information Act, Chapter 552, Texas Government Code.

5.7 **Publications.** All published material and written reports submitted under the Contract must be originally developed material unless otherwise specifically provided in the Contract. When material not originally developed is included in a report in any form, the source shall be identified.

SECTION 6. WARRANTIES

6.1 **Warranty – Price.**

The Contractor certifies that the prices in the Offer have been arrived at independently without consultation, communication, or agreement for the purpose of restricting competition, as to any matter relating to such fees with any other firm or with any competitor.

6.2 **Warranty – Title.**

The Contractor warrants that it has good and indefeasible title to all Deliverables furnished under the Contract, and that the Deliverables are free and clear of all liens, claims, security interests and encumbrances. The Contractor shall indemnify and hold the City harmless from and against all adverse title claims to the Deliverables.

6.3 **<u>Warranty – Deliverables</u>.** The Contractor warrants and represents that all Deliverables sold the City under the Contract shall be free from defects in design, workmanship or manufacture, and conform in all material respects to the specifications, drawings, and descriptions in the Solicitation, to any samples furnished by the Contractor, to the terms, covenants and conditions of the Contract, and to all applicable State, Federal or local laws, rules, and regulations, and industry codes and standards. Unless otherwise stated in the Solicitation, the Deliverables shall be new or recycled merchandise, and not used or reconditioned.

6.3.1 Recycled Deliverables shall be clearly identified as such.

6.3.2 The Contractor may not limit, exclude or disclaim the foregoing warranty or any warranty implied by law; and any attempt to do so shall be without force or effect.

6.3.3 Unless otherwise specified in the Contract, the warranty period shall be at least one year from the date of acceptance of the Deliverables or from the date of acceptance of any replacement Deliverables. If during the warranty period, one or more of the above warranties are breached, the Contractor shall promptly upon receipt of demand either repair the non-conforming Deliverables, or replace the non-conforming Deliverables with fully conforming Deliverables, at the City's option and at no additional cost to the City. All costs incidental to such repair or replacement, including but not limited to, any packaging and shipping costs, shall be borne exclusively by the Contractor. The City shall endeavor to give the Contractor written notice of the breach of warranty within thirty (30) calendar days of discovery of the breach of warranty, but failure to give timely notice shall not impair the City's rights under this section.

6.3.4 If the Contractor is unable or unwilling to repair or replace defective or non-conforming Deliverables as required by the City, then in addition to any other available remedy, the City may reduce the quantity of Deliverables it may be required to purchase under the Contract from the Contractor, and purchase conforming Deliverables from other sources. In such event, the Contractor shall pay to the City upon demand the increased cost, if any, incurred by the City to procure such Deliverables from another source.

6.3 If the Contractor is not the manufacturer, and the Deliverables are covered by a separate manufacturer's warranty, the Contractor shall transfer and assign such manufacturer's warranty to the City. If for any reason the manufacturer's warranty cannot be fully transferred to the City, the Contractor shall assist and cooperate with the City to the fullest extent to enforce such manufacturer's warranty for the benefit of the City.

6.4 **<u>Warranty – Services</u>.** The Contractor warrants and represents that all services to be provided the City under the Contract will be fully and timely performed in a good and workmanlike manner in accordance with generally accepted industry standards and practices, the terms, conditions, and covenants of the Contract, and all applicable Federal, State and local laws, rules or regulations.

6.4.1 The Contractor may not limit, exclude or disclaim the foregoing warranty or any warranty implied by law, and any attempt to do so shall be without force or effect.

6.4.2 Unless otherwise specified in the Contract, the warranty period shall be <u>at least</u> one year from the Acceptance Date. If during the warranty period, one or more of the above warranties are breached, the Contractor shall promptly upon receipt of demand perform the services again in accordance with above standard at no additional cost to the City. All costs incidental to such additional performance shall be borne by the Contractor. The City shall endeavor to give the Contractor written notice of the breach of warranty within thirty (30) calendar days of discovery of the breach warranty, but failure to give timely notice shall not impair the City's rights under this section.

6.4.3 If the Contractor is unable or unwilling to perform its services in accordance with the above standard as required by the City, then in addition to any other available remedy, the City may reduce the amount of services it may be required to purchase under the Contract from the Contractor, and purchase conforming services from other sources. In such event, the Contractor shall pay to the City upon demand the increased cost, if any, incurred by the City to procure such services from another source.

6.5 **NO WARRANTY BY CITY AGAINST INFRINGEMENTS**: The Contractor represents and warrants to the City that: (i) the Contractor shall provide the City good and indefeasible title to the Deliverables and (ii) the Deliverables supplied by the Contractor in accordance with the specifications in the Contract will not infringe, directly or contributorily, any United States patent, trademark, copyright, trade secret, or any other intellectual property right of any kind of any third party; that no claims have been made by any person or entity with respect to the ownership or operation of the Deliverables and the Contractor does not know of any valid basis for any such claims. The Contractor shall, at its sole expense, defend, indemnify, and hold the City harmless from and against all liability, damages, and costs (including court costs and reasonable fees of attorneys and other professionals) arising out of or resulting from: (i) any claim that the City's exercise of the rights associated with the City's' ownership, and if applicable, license rights, and its use of the Deliverables infringes the intellectual property rights of any third party; or (ii) the Contractor's breach of any of Contractor's representations or warranties stated in this Contract. In the event of any such claim, the City shall have the right to monitor such claim or at its option engage its own separate counsel to act as co-counsel on the City's behalf. Further, Contractor agrees that the City's specifications regarding the Deliverables shall in no way diminish Contractor's warranties or obligations under this paragraph and the City makes no warranty that the production, development, or delivery of such Deliverables will not impact such warranties of Contractor. Contractor shall have no liability nor obligation to defend the City against any such infringement action that is based upon or arises out of; i) infringement by reason of the City's design or specification requirement or any design other than of Contractor, or, ii) the use or alteration of the subject Services, materials or equipment or any component thereof in combination with any other system, equipment or software that is: a) not otherwise supplied or specified by Contractor, or b) inconsistent with the indicated use of the Services, material and/or equipment or any component thereof. This defense and indemnification obligation shall be effective only if the City has made all payments then due hereunder and if Contractor is notified promptly in writing and given authority, information, and assistance from the City, at Contractor's expense, for the defense of the same. Without limiting the generality of this paragraph, in the event the use by City of Contractor supplied product is enjoined in such a suit, Contractor shall, at its expense and at its sole option, either; (i) procure the right for the City to continue using such product, or (ii) modify such product to render it non-infringing (provided such modification does not materially degrade the performance, functioning or operation of the product), or (iii) replace such product with non-infringing product, or (iv) refund or credit the amount paid by the City for the infringing product. Contractor will not be responsible for any compromise or settlement made without its written consent.

SECTION 7. MISCELLANEOUS

7.1 **CONTRACTOR TO PACKAGE DELIVERABLES**: The Contractor will package Deliverables in accordance with good commercial practice and shall include a packing list showing the description of each item, the quantity and unit price Unless otherwise provided in the Specifications or Supplemental Terms and Conditions, each shipping container shall be clearly and permanently marked as follows: (a) The Contractor's name and address, (b) the City's name, address and purchase order or purchase release number and the price agreement number if applicable, (c) Container number and total number of containers, e.g. box 1 of 4 boxes, and (d) the number of the container bearing the packing list. The Contractor shall bear cost of packaging. Deliverables shall be suitably packed to secure lowest transportation costs and to conform with requirements of common carriers and any applicable specifications. The City's count or weight shall be final and conclusive on shipments not accompanied by packing lists.

7.2 **SHIPMENT UNDER RESERVATION PROHIBITED**: The Contractor is not authorized to ship the Deliverables under reservation and no tender of a bill of lading will operate as a tender of Deliverables.

7.3 **TITLE & RISK OF LOSS**: Title to and risk of loss of the Deliverables shall pass to the City only when the City actually receives and accepts the Deliverables.

7.4 **DELIVERY TERMS AND TRANSPORTATION CHARGES**: Deliverables shall be shipped F.O.B. point of delivery unless otherwise specified in the Supplemental Terms and Conditions. Unless otherwise stated in the Offer, the Contractor's price shall be deemed to include all delivery and transportation charges. The City shall have the right to designate what method of transportation shall be used to ship the Deliverables. The place of delivery shall be that set forth in the block of the purchase order or purchase release entitled "Receiving Agency".

7.5 **RIGHT OF INSPECTION AND REJECTION**: The City expressly reserves all rights under law, including, but not limited to the Uniform Commercial Code, to inspect the Deliverables at delivery before accepting them, and to reject defective or non-conforming Deliverables. If the City has the right to inspect the Contractor's, or the Contractor's Subcontractor's, facilities, or the Deliverables at the Contractor's, or the Contractor's Subcontractor's, premises, the Contractor shall furnish, or cause to be furnished, without additional charge, all reasonable facilities and assistance to the City to facilitate such inspection.

7.6 **NO REPLACEMENT OF DEFECTIVE TENDER**: Every tender or delivery of Deliverables must fully comply with all provisions of the Contract as to time of delivery, quality, and quantity. Any non-complying tender shall constitute a breach and the Contractor shall not have the right to substitute a conforming tender; provided, where the time for performance has not yet expired, the Contractor may notify the City of the intention to cure and may then make a conforming tender within the time allotted in the contract.

7.7 **PLACE AND CONDITION OF WORK**: The City shall provide the Contractor access to the sites where the Contractor is to perform the services as required in order for the Contractor to perform the services in a timely and efficient manner, in accordance with and subject to the applicable security laws, rules, and regulations. The Contractor acknowledges that it has satisfied itself as to the nature of the City's service requirements and specifications, the location and essential characteristics of the work sites, the quality and quantity of materials, equipment, labor and facilities necessary to perform the services, and any other condition or state of fact which could in any way affect performance of the Contractor's obligations under the contract. The Contractor hereby releases and holds the City harmless from and against any liability or claim for damages of any kind or nature if the actual site or service conditions differ from expected conditions.

7.8 **WORKFORCE**

7.8.1 The Contractor shall employ only orderly and competent workers, skilled in the performance of the services which they will perform under the Contract.

7.8.2 The Contractor, its employees, subcontractors, and subcontractor's employees may not while engaged in participating or responding to a solicitation or while in the course and scope of delivering goods or services under a City of Austin contract or on the City's property.

7.8.2.1 use or possess a firearm, including a concealed handgun that is licensed under state law, except as required by the terms of the contract; or

7.8.2.2 use or possess alcoholic or other intoxicating beverages, illegal drugs or controlled substances, nor may such workers be intoxicated, or under the influence of alcohol or drugs, on the job.

7.8.3 If the City or the City's representative notifies the Contractor that any worker is incompetent, disorderly or disobedient, has knowingly or repeatedly violated safety regulations, has possessed any firearms, or has possessed or was under the influence of alcohol or drugs on the job, the Contractor shall immediately remove such worker from Contract services, and may not employ such worker again on Contract services without the City's prior written consent.

7.9 **WORKFORCE SECURITY CLEARANCE AND IDENTIFICATION (ID):**

7.9.1 Contractors are required to obtain a certified criminal background report with fingerprinting (referred to as the "report") for all persons performing on the contract, including all Contractor, Subcontractor, and Supplier personnel (for convenience referred to as "Contractor's personnel").

7.9.2 The report may be obtained by reporting to one of the below governmental entities, submitting to fingerprinting and requesting the report [requestors may anticipate a two-week delay for State reports and up to a four to six week delay for receipt of a Federal report.

7.9.3 Contractor shall obtain the reports at least 30 days prior to any onsite work commencement. Contractor also shall attach to each report the project name, Contractor's personnel name(s), current address(es), and a copy of the U.S. state-issued or foreign national driver's license or photo ID card.

7.9.4 Contractor shall provide the City a Certified Criminal Background Report affirming that Contractor has conducted required security screening of Contractor's personnel to determine those appropriate for execution of the work and for presence on the City's property. A list of all Contractor Personnel requiring access to the City's site shall be attached to the affidavit.

7.9.5 Upon receipt by the City of Contractor's affidavit described in (D) above and the list of the Contractor's personnel, the City will provide each of Contractor's personnel a contractor ID badge that is required for access to City property that shall be worn at all times by Contractor's personnel during the execution of the work.

7.9.6 The City reserves the right to deny an ID badge to any Contractor personnel for reasonable cause, including failure of a Criminal History background check. The City will notify the Contractor of any such denial no more than twenty (20) days after receipt of the Contractor's reports. Where denial of access by a particular person may cause the Contractor to be unable to perform any portion of the work of the contract, the Contractor shall so notify the City's Contract Manager, in writing, within ten (10) calendar days of the receipt of notification of denial.

7.9.7 Contractor's personnel will be required to wear the ID badge at all times while on the work site. Failure to wear or produce the ID badge may be cause for removal of an individual from the work site, without regard to Contractor's schedule. Lost ID badges shall be reported to the City's Contract Manager. Contractor shall reimburse the City for all costs incurred in providing additional ID badges to Contractor Personnel.

7.9.8 ID badges to enter and/or work on the City property may be revoked by the City at any time. ID badges must be returned to the City at the time of project completion and acceptance or upon removal of an individual from the work site.

7.9.9 Contractor is not required to obtain reports for delivery personnel, including but not limited to FedEx, UPS, Roadway, or other materials delivery persons, however all delivery personnel must present company/employer-issued photo ID and be accompanied by at least one of Contractor's personnel at all times while at the work site.

7.9.10 The Contractor shall retain the reports and make them available for audit by the City during regular business hours (reference paragraph 17 in Section 0300, entitled Right to Audit).

7.10 **SPECIAL TOOLS & TEST EQUIPMENT**: If the price stated on the Offer includes the cost of any special tooling or special test equipment fabricated or required by the Contractor for the purpose of filling this order, such special tooling equipment and any process sheets related thereto shall become the property of the City and shall be identified by the Contractor as such.

7.11 **Right To Audit**.

7.11.1 The Contractor agrees that the representatives of the Office of the City Auditor or other authorized representatives of the City shall have access to, and the right to audit, examine, or reproduce, any and all records of the Contractor related to the performance under this Contract. The Contractor shall retain all such records for a period of three (3) years after final payment on this Contract or until all audit and litigation matters that the City has brought to the attention of the Contractor are resolved, whichever is longer. The Contractor agrees to refund to the City any overpayments disclosed by any such audit.

7.11.2 The Contractor shall include section a. above in all subcontractor agreements entered into in connection with this Contract.

7.12 **Stop Work Notice**. The City may issue an immediate Stop Work Notice in the event the Contractor is observed performing in a manner that is in violation of Federal, State, or local guidelines, or in a manner that is determined by the City to be unsafe to either life or property. Upon notification, the Contractor will cease all work until notified by the City that the violation or unsafe condition has been corrected. The Contractor shall be liable for all costs incurred by the City as a result of the issuance of such Stop Work Notice.

7.13 **Indemnity**.

7.13.1 Definitions:

7.13.1.1 "Indemnified Claims" shall include any and all claims, demands, suits, causes of action, judgments and liability of every character, type or description, including all reasonable costs and expenses of litigation, mediation or other alternate dispute resolution mechanism, including reasonable attorney and other professional fees for:

7.13.1.1.1 damage to or loss of the property of any person (including, but not limited to the City, the Contractor, their respective agents, officers, employees and subcontractors; the officers, agents, and employees of such subcontractors; and third parties); and/or;

7.13.1.1.2 death, bodily injury, illness, disease, worker's compensation, loss of services, or loss of income or wages to any person (including but not limited to the agents, officers and employees of the City, the Contractor, the Contractor's subcontractors, and third parties),

7.13.1.2 "Fault" shall include the sale of defective or non-conforming Deliverables, negligence, willful misconduct, or a breach of any legally imposed strict liability standard.

7.13.2 **THE CONTRACTOR SHALL DEFEND (AT THE OPTION OF THE CITY, IN ITS REASONABLE DISCRETION), INDEMNIFY, AND HOLD THE CITY, ITS SUCCESSORS, ASSIGNS, OFFICERS, EMPLOYEES AND ELECTED OFFICIALS HARMLESS FROM AND AGAINST ALL INDEMNIFIED CLAIMS DIRECTLY ARISING OUT OF, INCIDENT TO, CONCERNING OR RESULTING FROM THE EXTENT OF THE FAULT OF THE CONTRACTOR, OR THE CONTRACTOR'S AGENTS, EMPLOYEES OR SUBCONTRACTORS, IN THE PERFORMANCE OF THE CONTRACTOR'S OBLIGATIONS UNDER THE CONTRACT. NOTHING HEREIN SHALL BE DEEMED TO LIMIT THE RIGHTS OF THE CITY OR THE CONTRACTOR (INCLUDING, BUT NOT LIMITED TO, THE RIGHT TO SEEK CONTRIBUTION) AGAINST ANY THIRD PARTY WHO MAY BE LIABLE FOR AN INDEMNIFIED CLAIM.** The foregoing indemnification and defense obligations are subject to an indemnified party providing Contractor with written notice of any such claim or liability within thirty (30) days after receipt by the indemnified party of its receipt of the written assertion of such claim, loss or liability, and, at Contractor's expense, all information and cooperation reasonably requested by Contractor to carry out its obligations under this provision. Furthermore, the obligation to defend and indemnify shall cease to apply to a claim to the proportional extent caused by the actions or inactions or other fault attributable to an indemnified party as established by agreement of the parties, or by a final and binding legal determination, in which event such indemnified party shall pay the claimant directly in satisfaction of such indemnified party's liability and reimburse Contractor all amounts reasonably incurred or paid by Contractor in defense or satisfaction of such indemnified party's liability. If Contractor fails to assume the defense, the City shall have the right to assume and control the defense with counsel of its own choice and all direct costs of such defense shall be charged to Contractor in addition to any indemnified losses.

7.14 **WAIVER OF CONSEQUENTIAL DAMAGES AND LIMITATION OF LIABLIITY. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, NEITHER PARTY, ITS OFFICERS, DIRECTORS, AFFILIATES OR EMPLOYEES, SHALL BE LIABLE TO THE OTHER FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGE OF ANY KIND WHATSOEVER, INCLUDING, WITHOUT LIMITATION, CLAIMS OF LOSS OF USE, DATA, PROFITS OR REVENUE OR OTHER ECONOMIC LOSS, REGARDLESS OF THE FORM OF ACTION OR THE THEORY OF RECOVERY, EVEN IF THE PARTY HAS BEEN APPRISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any other provision of this Agreement and to the extent permitted by applicable law, the maximum liability of Contractor with respect to direct damages incurred by the City, whether in contract, in tort (including negligence or strict liability) or otherwise, is limited to the Contract price, excluding claims based upon the gross negligence or intentional misconduct of Contractor.**

7.15 **Claims.** If any claim, demand, suit, or other action is asserted against the Contractor which arises under or concerns the Contract, or which could have a material adverse affect on the Contractor's ability to perform thereunder, the Contractor shall give written notice thereof to the City within ten (10) calendar days after receipt of notice by the Contractor. Such notice to the City shall state the date of notification of any such claim, demand, suit, or other action; the names and addresses of the claimant(s); the basis thereof; and the name of each person against whom such claim is being asserted. Such notice shall be delivered personally or by mail and shall be sent to the City and to the Austin City Attorney. Personal delivery to the City Attorney shall be to City Hall, 301 West 2nd Street, 4th Floor, Austin, Texas 78701, and mail delivery shall be to P.O. Box 1088, Austin, Texas 78767.

7.16 **Notices.** Unless otherwise specified, all notices, requests, or other communications required or appropriate to be given under the Contract shall be in writing and shall be deemed delivered three (3) business days after postmarked if sent by U.S. Postal Service Certified or Registered Mail, Return Receipt Requested. Notices delivered by other means shall be deemed delivered upon receipt by the addressee. Routine communications may be made by first class mail, telefax, or other commercially accepted means. Notices to the Contractor shall be sent to the address specified in the Contractor's Offer, or at such other address as a party may notify the other in writing. Notices to the City shall be addressed to the City at P.O. Box 1088, Austin, Texas 78767 and marked to the attention of the Contract Administrator.

7.17 **Confidentiality.** In order to provide the Deliverables to the City, Contractor may require access to certain of the City's and/or its licensors' confidential information (including inventions, employee information, trade secrets, confidential know-how, confidential business information, and other information which the City or its licensors consider confidential) (collectively, "Confidential Information"). Contractor acknowledges and agrees that the Confidential Information is the valuable property of the City and/or its licensors and any unauthorized use, disclosure, dissemination, or other release of the Confidential Information will substantially injure the City and/or its licensors. The Contractor (including its employees, subcontractors, agents, or representatives) agrees that it will maintain the Confidential Information in strict confidence and shall not disclose, disseminate, copy, divulge, recreate, or otherwise use the Confidential Information without the prior written consent of the City or in a manner not expressly permitted under this Agreement, unless the Confidential Information is required to be disclosed by law or an order of any court or other governmental authority with proper jurisdiction, provided the Contractor promptly notifies the City before disclosing such information so as to permit the City reasonable time to seek an appropriate protective order. The Contractor agrees to use protective measures no less stringent than the Contractor uses within its own business to protect its own most valuable information, which protective measures shall under all circumstances be at least reasonable measures to ensure the continued confidentiality of the Confidential Information. Information shall not be deemed confidential if it is; publically available prior to this Contract or is subsequently made publicly available, rightfully received by the Contractor from a third party without accompanying confidentiality obligations, already in the Contractor's possession and was lawfully received from sources other than the City, independently developed by the Contractor or approved by the City for release.

7.18 **NON-SOLICITATION**:

7.18.1 During the term of the Contract, and for a period of six (6) months following termination of the Contract, the Contractor, its affiliate, or its agent shall not hire, employ, or solicit for employment or consulting services, a City employee employed in a technical job classification in a City department that engages or uses the services of a Contractor employee.

7.18.2 In the event that a breach of Paragraph A occurs the Contractor shall pay liquidated damages to the City in an amount equal to the greater of: (i) one (1) year of the employee's annual compensation; or (ii) 100 percent of the employee's annual compensation while employed by the City.

7.18.3 During the term of the Contract, and for a period of six (6) months following termination of the Contract, a department that engages the services of the Contractor or uses the services of a Contractor employee will not hire a Contractor employee while the employee is performing work under a Contract with the City unless the City first obtains the Contractor's approval.

7.18.4 In the event that a breach of Paragraph C occurs, the City shall pay liquidated damages to the Contractor in an amount equal to the greater of: (i) one (1) year of the employee's annual compensation or (ii) 100 percent of the employee's annual compensation while employed by the Contractor.

7.19 **Advertising.** The Contractor shall not advertise or publish, without the City's prior consent, the fact that the City has entered into the Contract, except to the extent required by law.

7.20 **No Contingent Fees.** The Contractor warrants that no person or selling agency has been employed or retained to solicit or secure the Contract upon any agreement or understanding for commission, percentage, brokerage, or contingent fee, excepting bona fide employees of bona fide established commercial or selling agencies maintained by the Contractor for the purpose of securing business. For breach or violation of this warranty, the City shall have the right, in addition to any other remedy available, to cancel the Contract without liability and to deduct from any amounts owed to the Contractor, or otherwise recover, the full amount of such commission, percentage, brokerage or contingent fee.

7.21 **Gratuities.** The City may, by written notice to the Contractor, cancel the Contract without liability if it is determined by the City that gratuities were offered or given by the Contractor or any agent or representative of the Contractor to any officer or employee of the City of Austin with a view toward securing the Contract or securing favorable treatment with respect to the awarding or amending or the making of any determinations with respect to the performing of such contract. In the event the Contract is canceled by the City pursuant to this provision, the City shall be entitled, in addition to any other rights and remedies, to recover or withhold the amount of the cost incurred by the Contractor in providing such gratuities.

7.22 **Prohibition Against Personal Interest in Contracts.** No officer, employee, independent consultant, or elected official of the City who is involved in the development, evaluation, or decision-making process of the performance of any solicitation shall have a financial interest, direct or indirect, in the Contract resulting from that solicitation. Any willful violation of this section shall constitute impropriety in office, and any officer or employee guilty thereof shall be subject to disciplinary action up to and including dismissal. Any violation of this provision, with the knowledge, expressed or implied, of the Contractor shall render the Contract voidable by the City.

7.23 **Independent Contractor.** The Contract shall not be construed as creating an employer/employee relationship, a partnership, or a joint venture. The Contractor's services shall be those of an independent contractor. The Contractor agrees and understands that the Contract does not grant any rights or privileges established for employees of the City.

7.24 **Assignment-Delegation.** The Contract shall be binding upon and enure to the benefit of the City and the Contractor and their respective successors and assigns, provided however, that no right or interest in the Contract shall be assigned and no obligation shall be delegated by the Contractor without the prior written consent of the City. Any attempted assignment or delegation by the Contractor shall be void unless made in conformity with this paragraph. The Contract is not intended to confer rights or benefits on any person, firm or entity not a party hereto; it being the intention of the parties that there be no third party beneficiaries to the Contract.

7.25 **Waiver.** No claim or right arising out of a breach of the Contract can be discharged in whole or in part by a waiver or renunciation of the claim or right unless the waiver or renunciation is supported by consideration and is in writing signed by the aggrieved party. No waiver by either the Contractor or the City of any one or more events of default by the other party shall operate as, or be construed to be, a permanent waiver of any rights or obligations under the Contract, or an express or implied acceptance of any other existing or future default or defaults, whether of a similar or different character.

7.26 **Modifications.** The Contract can be modified or amended only by a writing signed by both parties. No pre- printed or similar terms on any the Contractor invoice, order or other document shall have any force or effect to change the terms, covenants, and conditions of the Contract.

7.27 **Interpretation.** The Contract is intended by the parties as a final, complete and exclusive statement of the terms of their agreement. No course of prior dealing between the parties or course of performance or usage of the trade shall be relevant to supplement or explain any term used in the Contract. Although the Contract may have been substantially drafted by one party, it is the intent of the parties that all provisions be construed in a manner to be fair to both parties, reading no provisions more strictly against one party or the other. Whenever a term defined by the Uniform Commercial Code, as enacted by the State of Texas, is used in the Contract, the UCC definition shall control, unless otherwise defined in the Contract.

7.28 **Dispute Resolution.**

7.28.1 If a dispute arises out of or relates to the Contract, or the breach thereof, the parties agree to negotiate prior to prosecuting a suit for damages. However, this section does not prohibit the filing of a lawsuit to toll the running of a statute of limitations or to seek injunctive relief. Either party may make a written request for a meeting between representatives of each party within fourteen (14) calendar days after receipt of the request or such later period as agreed by the parties. Each party shall include, at a minimum, one (1) senior level individual with decision-making authority regarding the dispute. The purpose of this and any subsequent meeting is to attempt in good faith to negotiate a resolution of the dispute. If, within thirty (30) calendar days after such meeting, the parties have not succeeded in negotiating a resolution of the dispute, they will proceed directly to mediation as described below. Negotiation may be waived by a written agreement signed by both parties, in which event the parties may proceed directly to mediation as described below.

7.28.2 If the efforts to resolve the dispute through negotiation fail, or the parties waive the negotiation process, the parties may select, within thirty (30) calendar days, a mediator trained in mediation skills to assist with resolution of the dispute. Should they choose this option, the City and the Contractor agree to act in good faith in the selection of the mediator and to give consideration to qualified individuals nominated to act as mediator. Nothing in the Contract prevents the parties from relying on the skills of a person who is trained in the subject matter of the dispute or a contract interpretation expert. If the parties fail to agree on a mediator within thirty (30) calendar days of initiation of the mediation process, the mediator shall be selected by the Travis County Dispute Resolution Center (DRC). The parties agree to participate in mediation in good faith for up to thirty (30) calendar days from the date of the first mediation session. The City and the Contractor will share the mediator's fees equally and the parties will bear their own costs of participation such as fees for any consultants or attorneys they may utilize to represent them or otherwise assist them in the mediation.

7.29 **Minority And Women Owned Business Enterprise (MBE/WBE) Procurement Program.**

7.29.1 All City procurements are subject to the City's Minority-Owned and Women-Owned Business Enterprise Procurement Program found at Chapters 2-9A, 2-9B, 2-9C and 2-9D of the City Code. The Program provides Minority-Owned and Women-Owned Business Enterprises (MBEs/WBEs) full opportunity to participate in all City contracts.

7.29.2 The City of Austin has determined that no goals are appropriate for this Contract. **Even though no goals have been established for this Contract, the Contractor is required to comply with the City's MBE/WBE Procurement Program, Chapters 2-9A, 2-9B, 2-9C and 2-9D, of the City Code, as applicable, if areas of subcontracting are identified.**

7.29.3 If any service is needed to perform the Contract and the Contractor does not perform the service with its own workforce or if supplies or materials are required and the Contractor does not have the supplies or materials in its inventory, the Contractor shall contact the Department of Small and Minority Business Resources (DSMBR) at (512) 974-7600 to obtain a list of MBE and WBE firms available to perform the service or provide the supplies or materials. The Contractor must also make a Good Faith Effort to use available MBE and WBE firms. Good Faith Efforts include but are not limited to contacting the listed MBE and WBE firms to solicit their interest in performing on the Contract; using MBE and WBE firms that have shown an interest, meet qualifications, and are competitive in the market; and documenting the results of the contacts.

7.30 **Subcontractors.**

7.30.1 If the Contractor identified Subcontractors in an MBE/WBE Program Compliance Plan or a No Goals Utilization Plan the Contractor shall comply with the provisions of Chapters 2-9A, 2-9B, 2-9C, and 2-9D, as applicable, of the Austin City Code and the terms of the Compliance Plan or Utilization Plan as approved by the City (the "Plan"). The Contractor shall not initially employ any Subcontractor except as provided in the Contractor's Plan. The Contractor shall not substitute any Subcontractor identified in the Plan, unless the substitute has been accepted by the City in writing in accordance with the provisions of Chapters 2-9A, 2-9B, 2-9C and 2-9D, as applicable. No acceptance by the City of any Subcontractor shall constitute a waiver of any rights or remedies of the City with respect to defective Deliverables provided by a Subcontractor. If a Plan has been approved, the Contractor is additionally required to submit a monthly Subcontract Awards and Expenditures Report to the Contract Manager and the Purchasing Office Contract Compliance Manager no later than the tenth calendar day of each month.

7.30.2 Work performed for the Contractor by a Subcontractor shall be pursuant to a written contract between the Contractor and Subcontractor. The terms of the subcontract may not conflict with the terms of the Contract, and shall contain provisions that:

7.30.2.1 require that all Deliverables to be provided by the Subcontractor be provided in strict accordance with the provisions, specifications and terms of the Contract;

7.30.2.2 prohibit the Subcontractor from further subcontracting any portion of the Contract without the prior written consent of the City and the Contractor. The City may require, as a condition to such further subcontracting, that the Subcontractor post a payment bond in form, substance and amount acceptable to the City;

7.30.2.3 require Subcontractors to submit all invoices and applications for payments, including any claims for additional payments, damages or otherwise, to the Contractor in sufficient time to enable the Contractor to include same with its invoice or application for payment to the City in accordance with the terms of the Contract;

7.30.2.4 require that all Subcontractors obtain and maintain, throughout the term of their contract, insurance in the type and amounts specified for the Contractor, with the City being named as an additional insured under the Commercial General Liability policy with respect to liability arising out of the operations performed by or on behalf of Contractor on behalf of City where required by written contract and allowed by law; and

7.30.2.5 require that the Subcontractor indemnify and hold the City harmless to the same extent as the Contractor is required to indemnify the City.

7.30.3 The Contractor shall be fully responsible to the City for all acts and omissions of the Subcontractors just as the Contractor is responsible for the Contractor's own acts and omissions. Nothing in the Contract shall create for the benefit of any such Subcontractor any contractual relationship between the City and any such Subcontractor, nor shall it create any obligation on the part of the City to pay or to see to the payment of any moneys due any such Subcontractor except as may otherwise be required by law.

7.30.4 The Contractor shall pay each Subcontractor its appropriate share of payments made to the Contractor not later than ten (10) calendar days after receipt of payment from the City.

7.31 **BUY AMERICAN ACT-SUPPLIES (Applicable to certain Federally funded requirements)**

7.31.1 Definitions. As used in this paragraph –

7.31.1.1 "Component" means an article, material, or supply incorporated directly into an end product.

7.31.1.2 "Cost of components" means –

7.31.1.2.1 For components purchased by the Contractor, the acquisition cost, including transportation costs to the place of incorporation into the end product (whether or not such costs are paid to a domestic firm), and any applicable duty (whether or not a duty-free entry certificate is issued); or

7.31.1.2.2 For components manufactured by the Contractor, all costs associated with the manufacture of the component, including transportation costs as described in paragraph (1) of this definition, plus allocable overhead costs, but excluding profit. Cost of components does not include any costs associated with the manufacture of the end product.

7.31.1.3 "Domestic end product" means-

7.31.1.3.1 An unmanufactured end product mined or produced in the United States; or

7.31.1.3.2 An end product manufactured in the United States, if the cost of its components mined, produced, or manufactured in the United States exceeds 50 percent of the cost of all its components. Components of foreign origin of the same class or kind as those that the agency determines are not mined, produced, or manufactured in sufficient and reasonably available commercial quantities of a satisfactory quality are treated as domestic. Scrap generated, collected, and prepared for processing in the United States is considered domestic.

7.31.1.4 "End product" means those articles, materials, and supplies to be acquired under the contract for public use.

7.31.1.5 "Foreign end product" means an end product other than a domestic end product.

7.31.1.6 "United States" means the 50 States, the District of Columbia, and outlying areas.

7.31.2 The Buy American Act (41 U.S.C. 10a - 10d) provides a preference for domestic end products for supplies acquired for use in the United States.

7.31.3 The City does not maintain a list of foreign articles that will be treated as domestic for this Contract; but will consider for approval foreign articles as domestic for this product if the articles are on a list approved by another Governmental Agency. The Offeror shall submit documentation with their Offer demonstrating that the article is on an approved Governmental list.

7.31.4 The Contractor shall deliver only domestic end products except to the extent that it specified delivery of foreign end products in the provision of the Solicitation entitled "Buy American Act Certificate".

7.32 **Jurisdiction And Venue.** The Contract is made under and shall be governed by the laws of the State of Texas, including, when applicable, the Uniform Commercial Code as adopted in Texas, V.T.C.A., Bus. & Comm. Code, Chapter 1, excluding any rule or principle that would refer to and apply the substantive law of another state or jurisdiction. All issues arising from this Contract shall be resolved in the courts of Travis County, Texas and the parties agree to submit to the exclusive personal jurisdiction of such courts. The foregoing, however, shall not be construed or interpreted to limit or restrict the right or ability of the City to seek and secure injunctive relief from any competent authority as contemplated herein.

7.33 **Invalidity.** The invalidity, illegality, or unenforceability of any provision of the Contract shall in no way affect the validity or enforceability of any other portion or provision of the Contract. Any void provision shall be deemed severed from the Contract and the balance of the Contract shall be construed and enforced as if the Contract did not contain the particular portion or provision held to be void. The parties further agree to reform the Contract to replace any stricken provision with a valid provision that comes as close as possible to the intent of the stricken provision. The provisions of this section shall not prevent this entire Contract from being void should a provision which is the essence of the Contract be determined to be void.

7.34 **Holidays.** The following holidays are observed by the City:

Holiday	Date Observed
New Year’s Day	January 1
Martin Luther King, Jr.’s Birthday	Third Monday in January
President’s Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	July 4
Labor Day	First Monday in September
Veteran’s Day	November 11
Thanksgiving Day	Fourth Thursday in November
Friday after Thanksgiving	Friday after Thanksgiving
Christmas Eve	December 24
Christmas Day	December 25

If a Legal Holiday falls on Saturday, it will be observed on the preceding Friday. If a Legal Holiday falls on Sunday, it will be observed on the following Monday.

7.35 **Survivability of Obligations.** All provisions of the Contract that impose continuing obligations on the parties, including but not limited to the warranty, indemnity, and confidentiality obligations of the parties, shall survive the expiration or termination of the Contract.

7.36 **Non-Suspension or Debarment Certification.** The City of Austin is prohibited from contracting with or making prime or sub-awards to parties that are suspended or debarred or whose principals are suspended or debarred from Federal, State, or City of Austin Contracts. By accepting a Contract with the City, the Vendor certifies that its firm and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the General Services Administration List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

7.37 **Incorporation of Documents. Section 0100, Standard Purchase Definitions**, is hereby incorporated into this Contract by reference, with the same force and effect as if they were incorporated in full text. The full text versions of this Section are available, on the Internet at the following online address: `http://www.austintexas.gov/sites/default/files/files/Finance/Purchasing/standard-purchase-definitions.pdf`.

7.38 **Order of Precedence.** The Contract includes, without limitation, the Solicitation, the Offer submitted in response to the Solicitation, the Contract award, the Standard Purchase Terms and Conditions, Supplemental Terms and Conditions if any, Specifications, and any addenda and amendments thereto. Any inconsistency or conflict in the Contract documents shall be resolved by giving precedence in the following order.

7.38.1 any exceptions to the Offer accepted in writing by the City;

7.38.2 the Supplemental Purchase Terms and Conditions;

7.38.3 the Standard Purchase Terms and Conditions;

7.38.4 the Offer and exhibits; within the Offer, drawings (figured dimensions shall govern over scaled dimensions) will take precedence over specifications or scope of work.

In witness whereof, the parties have caused duly authorized representatives to execute this Contract on the dates set forth below.

Schneider Electric Buildings Americas, Inc.
By:
Signature
Name: John C Collins
Printed Name
Title: VP South Region
Date: 7-30-14

CITY OF AUSTIN
By: Michael Benson
Signature
Name: Michael Benson
Printed Name
Title: Chief Administrative Officer
Date: 8-1-2014

EXHIBIT A
Pricing Agreement and Scope of Work

Pricing under this contract will be determined according to the U.S. General Services Administration pricing schedule. (https://www.gsaadvantage.gov)

If any product or service is not found on GSA pricing schedule, then pricing shall be no less than 10% off the MSRP for these products or services.

CITY OF AUSTIN, TEXAS

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS)

STATEMENT OF OBJECTIVES

Version 0.1

[Date published]

Statement of Objectives

---

1 Purpose

1.1 The purpose of this solicitation is to obtain the following services in support of the City of Austin's existing installations of Schneider Electric Electronic Security Systems (ESS):

a) **Software maintenance and support** for installed instances of Schneider Electric Continuum software, both in-warranty and out-of-warranty. (Ref: section 2.1 below)

b) **Hardware maintenance and support** for components installed by Schneider Electric Corp., both in-warranty and out-of-warranty. (Ref: section 2.2 below)

c) **Design and installation** of new software and hardware components for purposes of expanding/adding to existing installations as requested by participating City Departments during the Contract Term. (Ref: section 2.3 below)

1.2 For the purposes of this Contract, ESS is defined as including:

- Physical Access Control System, hereinafter referred to as PACS;
- Intrusion Detection System, hereinafter referred to as IDS;
- Intercommunications System, hereinafter referred to as Intercom;

- Video Assessment and Surveillance System, hereinafter referred to as VASS;
- Electronic Personal Protection System, hereinafter referred to as EPPS.

1.3 This Statement of Objectives (SOO) provides the City's objectives for the contract, and lists the services required of the Contractor to achieve the objectives. The performance measures and performance criteria for the contract are itemized in the Division 28 specifications (Attachment A).

1.4 Exclusions

a) Fire Detection and Alarm Systems, and integration of ESS to Fire Detection and Alarm Systems, are specifically excluded from the scope of this Contract.

b) Building Automation Systems, and integration of ESS to Building Automation Systems, are specifically excluded from the scope of this Contract.

2 Contract Objectives

The City's Objectives for this Contract are as follows:

2.1 Software Maintenance and Support

2.1.1 Maintain reliability and continuity of operations for existing ESS ***site installations*** (including software and firmware) by ensuring that there are no more than 4 hours of unscheduled down time per year for any site (based on 365 days, 24 hours per day);

2.1.2 Maintain reliability and continuity of operations for the ***enterprise ESS components*** (workstations, servers and software) by ensuring that there are no more than 4 hours of unscheduled down time per year for any site (based on 365 days, 24 hours per day);

2.1.3 Keep the Continuum ESS system current with software and firmware revisions;

2.1.4 Create and utilize clearly defined method and processes for reporting system and component problems and failures;

2.1.5 Deliver same-business-day and next-business-day repair or replacement of inoperative hardware or software at standard labor rates per the Contract;

2.1.6 Deliver emergency after-hours repair or replacement of inoperative hardware or software at after-hours labor rates per the Contract.

2.2 Hardware Maintenance and Support

2.2.1 Maintain reliability and continuity of operations for existing ESS ***site installations*** (including hardware components, cabling, electronic devices) by ensuring that there are no more than 4 hours of unscheduled down time per year for any site (based on 365 days, 24 hours per day);

2.2.2 Keep the Continuum ESS system current with software and firmware revisions;
2.2.3 Create and utilize clearly defined method and processes for reporting system and component problems and failures;
2.2.4 Deliver same-business-day and next-business-day repair or replacement of inoperative hardware or software at standard labor rates per the Contract;
2.2.5 Deliver emergency after-hours repair or replacement of inoperative hardware or software at after-hours labor rates per the Contract.

2.3 Design and Installation of New Software and Hardware Components

2.3.1 Expand **existing ESS site installations** with additional capacity and functionality as required by participating City departments per new Sub-Project Scopes of Work;
2.3.2 Create clearly defined methods and processes for the City to request new Sub-Project Scopes of Work for purposes of expanding or adding to existing installations;
2.3.3 Obtain design consulting services from the Contractor prior to issuing and approving new Sub-Project Scopes of Work;
2.3.4 Obtain project management services from the Contractor for new Sub-Project Scopes of Work;
2.3.5 Ensure that City-requested Sub-Project Scopes of Work are executed per the requesting Departments requirements.

3 Scope Statement

The Contractor will provide a full range of design, installation, testing and support services for the City's Schneider Electric ESS systems. This includes design consulting, hardware installation, hardware support, software installation, project management services, software support, system upgrades and maintenance, cabling installations for ESS, firmware installation, firmware support, system training, and system testing. The Contractor shall be authorized by the Schneider Electric Corporation to sell and support the Continuum security management software and all Schneider Electric products provided to the City under this Contract.

3.1 Participating City Departments

This Contract will allow participating City Departments to request new Requests for Quotations and to obtain support services for existing installations. Participating City Departments are:

3.1.1 Austin Convention Center Department
3.1.2 Austin/Travis County Emergency Medical Services Department
3.1.3 Austin Fire Department
3.1.4 Austin Police Department
3.1.5 Austin Public Library Department
3.1.6 Austin Resource Recovery Department
3.1.7 Austin Water Utility Department

3.1.8 Communications & Technology Management Department
3.1.9 Human Resources Department
3.1.10 Public Works Department

To achieve the City's Objectives stated above, the following services shall be provided by the Contractor:

3.2 Provide Consulting Services

The Contractor shall provide Consulting Services to the requesting City Department for the purpose of ensuring that the proposed design will meet the Department's security requirements. Consulting Services may include meetings, site walk-throughs/inspections, email correspondence, design drawings/sketches and information, and Quotations as needed to ensure that the Contractor and requesting Department have a common understanding of the design proposal. Consulting services labor hours shall be included in Contractor's Quotations, and shall invoiced in conjunction with the first agreed-upon milestone invoice. In the event that the requested work does not materialize or is not funded by the City, Contractor may invoice for the actual Design Consulting services labor hours incurred , or per the in Quotation, whichever is less.

3.2.1 Performance Standards for Consulting Services

See (attached) Division 28 05 00 COMMON WORK RESULTS, Part 3 EXECUTION, 3.1 COMMON REQUIREMENTS FOR DESIGN AND CONSULTING SERVICES.

3.3 Provide Installation Services

Upon approval by the requesting City Department, and after the City Department has issued a Delivery Order to the Contractor, the Contractor will install the system as designed, using in-house personnel and/or sub-contracted personnel.

3.3.1 Performance Standards for Installation Services

See (attached) Division 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 3 EXECUTION, 3.2 COMMON REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY INSTALLATION.

3.4 Provide System Testing, Commissioning and Acceptance

All installed ESS systems shall be tested by the Contractor to ensure that the system performs as designed and according to the requesting Department's requirements prior to presenting to the requesting Department for acceptance. When the system is presented to the requesting City Department for acceptance, Contractor shall demonstrate the functionality of the system to the Department's satisfaction prior to acceptance.

3.4.1 Performance Standards for System Testing

See (attached) 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 3, EXECUTION, Part 3 EXECUTION, 3.4 COMMISSIONING

AND

28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 3, EXECUTION, Part 3 EXECUTION, 3.8 TESTING AND ACCEPTANCE.

3.5 Provide Software Maintenance and Updates

All components of the Continuum ESS system must be kept current with software and firmware revisions, as required by the City. Contractor shall offer make software and firmware updates and upgrades available to the City as soon as they are available from the manufacturer. The City will negotiate with the Contractor for installation of updates and upgrades on a per-occurrence basis.

3.5.1 Performance Standards for Software Maintenance and Updates

See (attached) 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 3, EXECUTION, Part 1 GENERAL, 1.9 MAINTENANCE AND SERVICE.

3.6 Provide System Support Services

Contractor shall provide software and hardware trouble-shooting, break/fix, warranty replacement and out-of-warranty replacement services for faulty or failed software and hardware system components. Contractor shall also provide escalation procedures and higher-level support services for problems that cannot be resolved directly by the Contractor's staff.

3.6.1 Performance Standards for System Support Services

See (attached) 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 3, EXECUTION, Part 1 GENERAL, 1.9 MAINTENANCE AND SERVICE.

4 Background

The City of Austin contracted with Schneider Electric December, 2008, for a five-year Agreement to provide enterprise Electronic Security Systems. This original Contract was developed to satisfy a specific Scope of Work (to replace existing security systems for (4) City departments; Austin Water Utility, CTM, CTECC, and the Austin Convention Center). The original Contract expiration date was on Dec. 3, 2013, but was extended for (120) days on Nov. 26, 2013 and will expire on April 2, 2104.

This new Contract will be a Master Agreement available to all participating City Departments, and will not limited to a specific Scope of Work. This Contract will be utilized by participating City Departments as their needs arise, and new Sub-Project Scopes of Work will be initiated by the City of Austin, and negotiated by the City of Austin and the Contractor per occurrence, and will be executed under the terms of this new Contract.

Under the new Contract, the Contractor shall provide system Maintenance and Support Services (see 3.1 and 3.2 above) for the duration of the Contract Term, and all ensuing Contract optional terms.

5 Contract Duration

This Contract shall be binding for an initial period of (12) months, commencing on the signing date. The Contract may be extended, at the City's discretion, for up to (4) ensuing 12-month periods thereafter.

6 Procurement Methodology

6.1 Procuring Maintenance & Support Services

Each participating City Department will issue a City Delivery Order (DO) to the Contractor using Department funds. Each Department will estimate the DO amount required for out-of-warranty maintenance and support services, and will issue the DO as a "blanket" DO to be used as funding source for required maintenance & support services rendered by the Contractor. The Contractor will be furnished the list of issued DOs, and will invoice against the DOs for services rendered.

6.2 Procuring System Expansions and Additions

Each participating City Department (see list of participating Departments in section 4.1 above) shall issue to Contractor a Sub-Project Scopes of Work for any of the services listed above in Section 3, Scope Statement. Contractor shall provide an itemized Quotation in response to each Request. The requesting City Department will review the provided Quotation, negotiate changes (if needed) with the Contractor, and will either approve or decline the Quotation. Upon approval, the Department will issue a Delivery Order (DO) to the Contractor, and the Contractor shall deliver the services as described in the Quotation. The requesting Department will make payments to the Contractor based on milestones negotiated, and upon presentation by the Contractor to the Department of an accurate invoice, and upon acceptance by the requesting Department of the milestone completion(s).

6.2.1 Quotation Requirements

Each Quotation provided to the City in response to a City Request for Quotation shall include, at a minimum, the following information:

6.2.1.1 Contractor Name, letterhead, address
6.2.1.2 Name of the Requesting Department
6.2.1.3 Name of the person making the Request
6.2.1.4 Date of the Quotation
6.2.1.5 A unique Quotation Number, not duplicated at any time during the Contract Term

6.2.1.6 A descriptive title for the Quotation (i.e. "12 Month Out-of-Warranty Support Services for XYZ Department ESS System Installed at 123 Anywhere Street, Austin, TX"

6.2.1.7 The Contractor's Quotation shall be organized as follows:

a) Materials

This section is an itemized quotation for materials required to satisfy the Request. Contractor may bundle like or similar items into a single line item. Contractor may bundle sub-assemblies into a single line item if all components of the sub-assembly are necessary to form a complete, working unit. Contractor may bundle miscellaneous hardware items into a single line item (i.e. "Mounting hardware, screws, cable ties, pull strings, support hardware"). Each line item shall include a description, part number (if applicable), Quantity proposed, Unit Price and Extended Price.

b) Labor

This section is an itemized quotation for labor hours required to satisfy the Request. Contractor may bundle like or similar items into a single line item (i.e. "Installation Services, Technician Level II"). Each line item shall include a description, part number (if applicable), Quantity proposed, Unit Price and Extended Price.

c) Software

This section is an itemized quotation for software, software licenses, license dongles, database licenses, or any other software-related component required to satisfy the Request. Each line item shall include a description, part number (if applicable), Quantity proposed, Unit Price and Extended Price.

d) Sub-Contracted Items

This section is an itemized quotation for sub-contracted services included in the Quotation. Each line item shall include a description, part number (if applicable), Quantity proposed, Unit Price and Extended Price.

e) Statement of Work

This section consists of a summary-level Statement of Work that includes, at a minimum, the following information:

- *Description of the work to be performed by Contractor, what the Contractor will provide, what the City will provide, specific exclusions, limitations and constraints;*
- *Proposed schedule (if applicable) for the Work;*
- *Proposed Payment Milestones.*

6.3 Sub-Project Scopes of Work

Upon delivery of a Quotation by the Contractor in response to a City-initiated Sub-Project Scope of Work, and upon approval by the City of the Quotation, a new Sub-Project Scope of Work will begin. A Sub-Project Scope of Work can range from a single delivery of commodities or supplies, to a multi-month support services agreement, up to an extended installation of new components and software. For purposes of identification, a Sub-Project Scope of Work can be numbered and described exactly the same as the Contractor's Quotation.

7 Constraints

7.1 Network Security Constraints

Due to the sensitive nature of the security monitoring and control systems, network security is of great importance to the City. The following constraints will dictate products and system configuration for ESS:

7.1.1 IP-enabled devices must be subjected to a Nessus vulnerability scan, and all high-level vulnerabilities must be eliminated or corrected prior to attaching ESS devices to the production network.
7.1.2 If IP-enabled devices cannot pass the Nessus scan for high-level vulnerabilities, the City may provide a secured, private LAN that is reserved for ESS communications only. The ESS LAN may be secured with a security device that eliminates the possibility of intruders using the high-level vulnerabilities discovered by the Nessus scan.
7.1.3 IP-enabled devices must NOT be running HTTP, HTTPS, FTP, SFTP, Telnet, or remote terminal services, unless exceptions are approved by CTM Security.
7.1.4 [Other Security constraints here]

8 Compensation

Contractor shall be compensated on a per-request basis for the duration of the Contract, with total compensation not to exceed $xxx.xx for services, hardware, software and Contract-related expenses that are included with each Quotation.

8.1 Pricing

Pricing for labor, hardware and software will be derived from the Contractor's GSA pricing schedule, with applicable City of Austin discounts. The GSA schedule will serve as verifiable, published document, and will be incorporated into the Contract by reference. All City of Austin orders will be placed directly with the Contractor (not via GSA). In the event that Contractor's GSA contract expires during the term of this Contract, pricing will be based on the Contractor's most current GSA schedule in effect prior to expiration.

8.2 Milestone Payments

Depending on the nature of the work requested by the City to be performed by the Contractor, milestone payments shall be proposed by Contractor in the Quotation, and may be negotiated by the City and the Contractor. Orders for commodity supplies, consumables and other goods not associated with a Scope of Work shall be invoiced singly by the Contractor following delivery acceptance to the requesting City Department. No payments will be made by the City to the Contractor without prior approval by the requesting City Department.

8.3 Pricing Increases

Contractor may request price adjustments annually, following the first (12) months of the signing date of the Contract. Price adjustments may be made using the U.S. Department of Labor Consumer Price Index ("Index") for U.S. City Average as a basis for the request.

8.3.1 Requests for price increases must be made in writing and submitted to the City of Austin Purchasing Buyer. The request must be signed by a Contractor employee with the authority to bind the Contractor contractually, shall reference the Contract number, and shall include the following:

8.3.1.1 An itemized, revised price list showing the previous pricing and the proposed increase per item, along with the effective proposed date of the increases;
8.3.1.2 A copy of the "Index" with the effective date of the "Index" clearly shown;
8.3.1.3 Copies of documentation, if applicable, that provide evidence of price increases from third-party suppliers that necessitate a corresponding price increase request from the Contractor.

9 Warranties

All materials and workmanship provided to City for each Scope of Work executed under this Contract must be warranted by the Contractor for a period of one (1) year following final acceptance of each Sub-Project Scope Of Work, even if manufacturer's materials warranties are of shorter duration. Defects found to be caused by faulty materials or workmanship shall be corrected by the Contractor at no cost to City. Examples of faulty workmanship might include mis-wired connections, improper mounting of devices or the failure of a system component to perform as design due to design flaws.

The period of Contractor's warranties for any items herein are not exclusive remedies, and the City has recourse to any warranties of additional scope transmitted by the Contractor to the City and all other remedies available at law or in equity.

10 Order of Precedence

For purposes of this Contract, the order of precedence in resolving performance contractual obligations and expectations are as follows:

1) Attachment A, City of Austin MasterFormat Division 28 Electronic Safety and Security specifications, which consists of the following documents:

   - 280500_CommonWorkResults.doc

  - 280513_ConductorsandCables.doc
  - 280526_GroundingandBonding.doc
  - 280800_Commissioning.doc
  - 281300_PhysicalAccessControl.doc
  - 281316_PhysicalAccessControlDatabase.doc
  - 281353_SecurityAccessDetection.doc
  - 281600_IntrusionDetection.doc
  - 282300_VideoSurveillance.doc

2) Section 2 of this document, Contract Objectives

3) Section 3 of this document, Scope Statement

4) Section 7 of this document, Constraints

~~11 Instructions to Contractor~~

~~11.1 Response Instructions~~

~~A. **Submit a Contract Statement of Work** - The Contractor shall use this document, along with all Attachments provided, as a basis for preparing a proposed **Contract Statement of Work (SOW)**. The Contract SOW shall provide the details of how the Contractor proposes to meet the City's objectives stated herein, how the Contractor proposes to provide the required services, and how the Contractor proposes to meet the performance measures.~~

~~B. **Submit a Pricing Proposal** – The Contractor shall prepare and submit a Pricing Proposal for all services and components specified herein.~~

~~1. Pricing for services rendered shall be submitted as an itemized schedule of prices for various types of labor rendered. For instance, the Services Pricing may include labor rates for various types of services and skill sets for standard business hours and for emergency after-hours. The Statement of Work shall specify days of the year and daily hours for both standard and after-hours.~~

~~2. Pricing for hardware and software components shall be based on a verifiable, standardized and published source of pricing information such as GSA schedule pricing or other government cooperative contract pricing, with applicable City of Austin discounts.~~

~~3. Pricing for custom items, one-off items and special work shall be provided to the City of Austin following the issuance of a Sub-Project Scope of Work request by the City of Austin to the Contractor. Such pricing will be negotiated by the City and the Contractor, and the City will provide approval and funding per Sub-Project.~~

~~C. The SOW shall be submitted, along with other required documents, with the Proposal, and will become the basis for Contract. The City, at its discretion, will choose to negotiate specific items provided in the SOW prior to Contract signing.~~

12 Acceptance and authorization

[Use the following format to create a signature page that confirms agreement of the products and services to be delivered, when, how, and for what price. Be sure to include any legal language as required by your company's legal representative. Get signatures of the client administrator, the Statement of Work author, and any other parties who are responsible for the SOW.]

The terms and conditions of the Contract apply in full to the services and products provided under this Statement of Objectives.

28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0, City of Austin, Texas

January, 2014

1 PART 1 - GENERAL

1.1 Description

A. This Section, Common Work Results, applies to all sections of Division 28.

B. The purpose of this solicitation is to obtain design, installation and support services for the City of Austin's existing and new installations of Schneider Electric Electronic Security Systems (ESS). For the purposes of this solicitation, ESS is defined as an integrated software solution providing a single point of control (per site) of various low-voltage security sub-systems, including electronic access control systems, video monitoring and recording systems, electronic intercom systems, burglar alarm systems, and intrusion detection systems.

C. Work to be provided shall include the following:

1. **Repair Services -** Replacement Parts On-site service during the warranty period shall be provided as specified herein under "1.9, F., Emergency Service". The Contractor shall guarantee all parts and labor for a term of one (1) year from date of Substantial Completion or Acceptance, whichever occurs first, unless dictated otherwise in this specification from the acceptance date of the system as described in Part 5 of this Specification. The Contractor shall be responsible for all equipment, software, shipping, transportation charges, and expenses associated with the warranty service of the system for one (1) year.
2. **Software Support Services -** The Contractor shall provide 24-hour telephone support for the software program at no additional charge to the owner. Software support shall include all software updates that occur during the warranty period.
3. **Design Services** – Contractor shall provide design consulting and advisory services for new or modified installations requested by the City of Austin. Services may include documents, meetings or telephone conversations as needed to fully specify ESS system components required to meet the objectives.
4. **Installation Services** – Contractor shall furnish and install fully functional electronic safety and security cabling system(s), equipment, and approved accessories in accordance with each sub-project specification section(s), drawing(s), and referenced publications. The Contractor shall provide a fully functional and operating ESS using the Andover Continuum system. The system

shall be programmed, configured, documented, and tested as required herein and by reference to related specification(s) documents. The Contractor shall provide calculations and analysis to support design and engineering decisions as specified in submittals. The Contractor shall provide and pay all labor, materials, and equipment, sales and gross receipts and other taxes. The Contractor shall secure and pay for plan check fees, permits, other fees, and licenses necessary for the execution of work as applicable for the project. The Contractor will comply with codes, ordinances, regulations, and other legal requirements of public authorities, which bear on the performance of work. The security system may include, depending on requirements and specifications for the ESS,: physical access control, intrusion detection, duress alarms, elevator control interface, video assessment and surveillance, video recording and storage, delayed egress, personal protection system, intercommunication system, equipment cabinetry, dedicated photo badging system and integrated live camera designed for use with the badging system, report printer, photo badge printer, and uninterruptible power supplies (UPS) interface. Operator training is required as part of the Contractor's scope and shall be provided by the Contractor. The Security Contractor shall be required to provide necessary maintenance and troubleshooting manuals as submittals as identified herein. The work shall include the procurement and installation of electrical wire and cables and the installation and testing of all system components. Inspection, testing, demonstration, and acceptance of equipment, software, materials, installation, documentation, and workmanship, shall be as specified herein. The Contractor shall provide all associated installation support, excluding the provision of primary electrical input power circuits.

5. **Training Services** – Contractor shall provide the following for new facilities and for major remodels of existing facilities:
    1. Site Familiarization Training **-** Training can include site familiarization training for CITY OF AUSTIN technicians and administrative personnel. Training shall include general information on new system layout including closet locations, turnover of the completed system including all documentation, including manuals, software, key systems, and full system administration rights. Lesson plans and training manuals training shall be oriented to type of training to be provided.
    2. New Unit Control Room Usage Training
        a) Provide the security personnel with training in the use, operation, and maintenance of the entire control room system (Unit Control and Equipment Rooms). The training documentation must include the operation and maintenance. The first of the training sessions shall take place prior to system turnover and the second immediately after turnover. Coordinate the training sessions with the City of Austin. Instruction is not to begin until the system is operational as designed.

        b) The training documents will cover the operation and the maintenance manuals and the control console operators' manuals and service manuals in detail, stressing all important operational and service diagnostic information necessary for the maintenance and operations personnel to efficiently use and maintain all systems.

        c) Provide an illustrated control console operator's manual and service manual. The operator's manual shall be written in laymen's language and printed so as to become a permanent reference document for the operators, describing all control panel switch operations, graphic symbol definitions and all indicating functions and a complete explanation of all software.

d) The service manual shall be written in laymen's language and printed so as to become a permanent reference document for maintenance personnel. The manual shall describe how to run internal self-diagnostic software programs, and how to troubleshoot head end hardware and field devices with a complete scenario simulation of all possible system malfunctions and the appropriate corrective measures.

D. Section Includes:

1. Description of Work for ESS
2. Electronic security equipment coordination with relating Divisions,
3. Submittal Requirements for Electronic Security,
4. Miscellaneous Supporting equipment and materials for Electronic Security,
5. Electronic security installation requirements.

1.2 Related Work

A. Section 08 71 00 - DOOR HARDWARE. Requirements for door installation.

B. Section 14 21 00 - ELECTRIC TRACTION ELEVATORS. Requirements for elevators.

C. Section 14 24 00 - HYDRAULIC ELEVATORS. Requirements for elevators Section 28 05 13

D. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

E. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

F. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.

G. Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. Requirements for Commissioning.

H. Section 28 13 00 - PHYSICAL ACCESS CONTROL SYSTEMS (PACS). For physical access control integration.

I. Section 28 13 16 - PHYSICAL ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT. Requirements for control and operation of all security systems.

J. Section 28 13 53 - SECURITY ACCESS DETECTION. Requirements for screening of personnel and shipments.

K. Section 28 16 00 - INTRUSION DETECTION SYSTEM (IDS). Requirements for alarm systems.

L. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

M. Section 28 26 00 - ELECTRONIC PERSONAL PROTECTION SYSTEM (EPPS). Requirements for emergency and interior communications.

N. Section 32 31 13 - CHAIN LINK FENCES AND GATES. Requirements for fences.

1.3 Definitions

A. AGC: Automatic Gain Control.

B. Basket Cable Tray: A fabricated structure consisting of wire mesh bottom and side rails.

C. BICSI: Building Industry Consulting Service International.

D. CCD: Charge-coupled device.

E. Central Station: A computer with software designated as the main controlling device for a building, campus or site for the security access system. Where this term is presented with initial capital letters, this definition applies.

F. Channel Cable Tray: A fabricated structure consisting of a one-piece, ventilated-bottom or solid-bottom channel section.

G. Controller: An intelligent peripheral control unit that uses a computer or CPU for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.

H. CPU: Central processing unit.

I. Credential: Data assigned to an entity and used to identify that entity.

J. DGP: Data Gathering Panel – component of the Physical Access Control System capable of communicating, storing and processing signals and information received from readers, reader modules, input modules, output modules, and Security Management System.

K. DTS: Digital Termination Service: A microwave-based, line-of-sight communications provided directly to the end user.

L. EMI: Electromagnetic interference.

M. EMT: Electric Metallic Tubing.

N. ESS: Electronic Security System.

O. File Server: A computer in a network that stores the programs and data files shared by users.

P. GFI: Ground fault interrupter.

Q. IDC: Insulation displacement connector.

R. Identifier: A credential card, keypad personal identification number or code, biometric characteristic, or other unique identification entered as data into the entry-control database for the purpose of identifying an individual. Where this term is presented with an initial capital letter, this definition applies.

S. I/O: Input/Output.

T. Intrusion Zone: A space or area for which an intrusion must be detected and uniquely identified, the sensor or group of sensors assigned to perform the detection, and any interface equipment between sensors and communication link to central-station control unit.

U. Ladder Cable Tray: A fabricated structure consisting of two longitudinal side rails connected by individual transverse members (rungs).

V. LAN: Local area network.

W. LCD: Liquid-crystal display.

X. LED: Light-emitting diode.

Y. Site: A structure or campus having control over its ESS systems. The Location may be stand-alone or may connected to the ESS enterprise system.

Z. Low Voltage: As defined in NFPA 70 for circuits and equipment operating at less than 50 V or for remote-control and signaling power-limited circuits.

AA. M-JPEG: Motion – Joint Photographic Experts Group.

AB. MPEG: Moving picture experts group.

AC. NEC: National Electric Code

AD. NEMA: National Electrical Manufacturers Association

AE. NFPA: National Fire Protection Association

AF. NTSC: National Television System Committee.

AG. NRTL: Nationally Recognized Testing Laboratory.

AH. Open Cabling: Passing telecommunications cabling through open space (e.g., between the studs of a wall cavity).

AI. PACS: Physical Access Control System; A system comprised of cards, readers, door controllers, servers and software to control the physical ingress and egress of people within a given space

AJ. PC: Personal computer. This acronym applies to the Central Station, workstations, and file servers.

AK. PCI Bus: Peripheral component interconnect; a peripheral bus providing a high-speed data path between the CPU and peripheral devices (such as monitor, disk drive, or network).

AL. PDF: (Portable Document Format.) The file format used by the Acrobat document exchange system software from Adobe.

AM. RCDD: BICSI Registered Communications Distribution Designer.

AN. RFI: Radio-frequency interference.

AO. RIGID: Rigid conduit is galvanized steel tubing, with a tubing wall that is thick enough to allow it to be threaded.

AP. RS-232: An TIA/EIA standard for asynchronous serial data communications between terminal devices. This standard defines a 25-pin connector and certain signal characteristics for interfacing computer equipment. Now known as TIA-232.

AQ. RS-485: An TIA/EIA standard for balanced, multipoint communications. Now known as TIA-485

AR. Solid-Bottom or Non-ventilated Cable Tray: A fabricated structure consisting of integral or separate longitudinal side rails, and a bottom without ventilation openings.

AS. SMS: Security Management System – A SMS is software that incorporates multiple security subsystems (e.g., physical access control, intrusion detection, closed circuit television, intercom) into a single platform and graphical user interface.

AT. SMS Server: A central computer with software designed to provide centralized services to one or more Central Stations distributed across a data network. Services may include communications processing, message format processing, data processing, data storage or other centralized functions.

AU. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

AV. Trough or Ventilated Cable Tray: A fabricated structure consisting of integral or separate longitudinal rails and a bottom having openings sufficient for the passage of air and using 75 percent or less of the plan area of the surface to support cables.

AW. UPS: Uninterruptible Power Supply

AX. UTP: Unshielded Twisted Pair

AY. Workstation: A PC with software that is configured for specific limited security system functions.

1.4 Quality Assurance

A. Pre-Qualified Manufacturers – subject to compliance with requirements, Contractor shall provide products supplied by the following pre-qualified manufacturers:

    1. Schneider Electric Andover Continuum
    2. Pelco VMS
    3. Zenith Intercom
    4. Bosch IDS
    5. Others as proposed and approved per sub-project

B. Contractor Qualifications

    1. The security Contractor or security sub-Contractor shall be a licensed security Contractor with a minimum of five (5) years of experience installing and servicing systems of similar scope and complexity. The Contractor shall be an authorized regional representative of the manufacturer (s).
    2. The Contractor shall only utilize factory-trained technicians to install, program, and service the City of Austin's security systems. The Contractor shall only utilize factory-trained technicians to install, terminate and service controller/field panels and reader modules. The technicians shall have a minimum of five (3) continuous years of technical experience in electronic security systems. The Contractor shall have a local service facility. The facility shall be located within [60] miles of the City of Austin downtown. The local facility shall include sufficient spare parts inventory to support the service requirements associated with this contract. The facility shall also include appropriate diagnostic equipment to perform diagnostic procedures. The City of Austin reserves the option of surveying the company's facility to verify the service inventory and presence of a local service organization.

C. Service Provider Qualifications

  1. There shall be a permanent service organization maintained or trained by the manufacturer which will render satisfactory service to this installation within four hours of receipt of notification that service is needed. Submit name and address of service organizations.

1.5 Submittals

A. The Contractor shall submit all items in accordance with the requirements of this specification. Provide (2) printed and (1) electronic copy of all submittal information. Submittals shall include the following items at a minimum:

  1. Overall system architecture showing conceptual design, quantity of devices and general location.
  2. Model numbers of all components furnished on the job.
  3. Manufacturer's installation instructions.
  4. Manufacturer's catalog data sheets for all components.
  5. Input power requirements for all components.
  6. Complete engineered drawings indicating:
     a. System layout – showing device locations on the facility drawings.
     b. Wiring diagrams including wiring paths.
     c. Device dimensions.
     d. Point-to-point wiring diagrams for all devices.
     e. Termination details for all devices.
     f. Single-line system architecture drawings representing the entire system.
     g. Door schedule for all doors equipped with electronic security components. Door schedule shall include:
        1) Door number (from A/E drawings)
        2) Lock type
        3) Card reader type and model
        4) Shunting device type and model (if applicable)
        5) Sounder type and model (if applicable)
        6) Other device types and models as required (such as delayed egress, electric transfer hinge, electronic pass-through device, etc.)
     h. Camera schedule that includes:
        1) Camera identifier (per drawings or per Customer)
        2) Camera location
        3) Camera type and model

            4) Mount type

7. System Configuration Package – Contractor shall provide documentation of the ESS system functionality and configuration that includes at least:
    a. Access levels
    b. System schedules (days and times of schedules for intrusion detection devices, physical access control devices, holiday schedules, burglar alarm schedules, etc.)
    c. Initial Access Badge database
    d. System monitoring and control details
    e. Naming conventions and descriptors
8. Performance Test Procedures – Contractor shall prepare and deliver to the City of Austin a set of Performance Test Procedures customized to the sub-project requirements.

1.6 Applicable Publications

The publications listed below (including amendments, addenda, revisions, supplement, and errata) form a part of this specification to the extent referenced. The publications are referenced in the text by the basic designation only.

A. National Electrical Code (NEC)
B. FCC Rules and Regulations
C. Part 15, Radio Frequency Devices
D. National Electrical Manufacturers Association (NEMA)
E. Applicable Federal, State and Local laws, regulations, codes
F. Americans with Disabilities Act (ADA)
G. NFPA 70 & 101
H. UL294
I. UL1076
J. Uniform Building Code – UBC
K. Local Authority Having Jurisdiction (AHJ)

1.7 Maintenance & service

1.7.1 Warranty

A. Period – Base Warranty Coverage
    1) The Contractor shall guarantee all labor, workmanship, and materials for a period of 1 year from the date of final acceptance. Should a failure occur within the first year, the Contractor shall provide all labor and materials necessary to restore the system to a complete operating condition, at no cost to the Owner.

2) Normal warranty repairs to be performed M-F, 8am to 5pm.

3) Provide (1) routine preventative maintenance inspection of the system prior to the base warranty expiration. Provide the client with a log of recommended service actions, correct any system deficiencies prior to the base warranty expiration.

4) Warranty coverage shall include those items provided and installed by the SMS contractor as well as the electronic components provided and installed by the division 8 contractor.

B. Optional Warranty – Extended Warranty Coverage

1) Provide the client with optional pricing as a part of the base bid. Pricing shall extend all services offered during the base warranty coverage period on an annual schedule. Provide pricing for warranty extension for 1, 2, 3, 4, and 5 years.

2) All extended warranty coverage's shall match the requirements of the base warranty coverage.

3) Provide line item unit pricing for:

  a. Local on-site training for system operators – 8 hour sessions.

  b. Factory based training – exclude travel costs.

1.7.2 General Requirements

A. The Contractor shall provide all services required and equipment necessary to maintain the entire integrated electronic security system in an operational state as specified for a period of one (1) year after formal written acceptance of the system. The Contractor shall provide all necessary material required for performing scheduled adjustments or other non-scheduled work. Impacts on facility operations shall be minimized when performing scheduled adjustments or other non-scheduled work. See also General Project Requirements.

1.7.3 Description of Work

A. The adjustment and repair of the security system includes all software updates, panel firmware, and the following new items: communications transmission equipment and data transmission media (DTM), local processors, security system sensors, physical access control equipment, facility interface, signal transmission equipment, and video equipment.

1.7.4 Personnel

A. Service personnel shall be certified in the maintenance and repair of the selected type of equipment and qualified to accomplish all work promptly and satisfactorily. The City of Austin will be advised in writing of the name of the designated service representative, and of any change in personnel. The City of Austin will be provided copies of system manufacturer certification for the designated service representative.

1.7.5 Schedule of Work

A. The work shall be performed during regular working hours, Monday through Friday, excluding federal holidays.

1.7.6 Emergency Service

A. The Owner shall initiate service calls whenever the system is not functioning properly. The Contractor shall provide the Owner with an emergency service center telephone number. The emergency service center shall be staffed 24 hours a day 365 days a year. The Owner shall have sole authority for determining catastrophic and non-catastrophic system failures within parameters stated in General Project Requirements.

1) For catastrophic system failures, the Contractor shall provide same day four (4) hour service response with a defect correction time not to exceed eight (8) hours from [notification] [arrival on site]. Catastrophic system failures are defined as any system failure that the Owner determines will place the facility(s) at increased risk.

2) For non-catastrophic failures, the Contractor within eight (8) hours with a defect correction time not to exceed 24 hours from notification.

1.7.7 Operation

A. Performance of scheduled adjustments and repair shall verify operation of the system as demonstrated by the applicable portions of the performance verification test.

1.7.8 Work Request

A. The Contractor shall separately record each service call request, as received. The record shall include the serial number identifying the component involved, its location, date and time the call was received, specific nature of trouble, names of service personnel assigned to the task, instructions describing the action taken, the amount and nature of the materials used, and the date and time of commencement and completion. The Contractor shall deliver a record of the work performed within five (5) working days after the work was completed.

1.7.9 System Modifications

A. The Contractor shall make any recommendations for system modification in writing to the City of Austin. No system modifications, including operating parameters and control settings, shall be made without prior written approval from the City of Austin. Any modifications made to the system shall be incorporated into the operation and maintenance manuals and other documentation affected.

1.7.10 Software Maintenance

A. The Contractor shall provide all software updates when approved by the Owner from the manufacturer during the installation and 12-month warranty period and verify operation of the system. These updates shall be accomplished in a timely manner, fully coordinated with the system operators, and incorporated into the operations and maintenance manuals and software documentation.

1.8 Systems Descriptions & Capabilities

1.8.1 Primary Function

A. The SMS's primary functions shall be to regulate access through specific doors and/or gates to secured areas of the Customer's site and facility and to provide digital DVMS recording capability to view live and recorded video that is associated with alarm events. The SMS shall utilize a single server for its access control with integration being provided using one operating environment. The SMS's workstation environment shall be a Microsoft Windows XP Workstation operating system. No alternates will be accepted.

B. The software architecture shall be object-oriented in design, a true 32 or 64 bit application suite utilizing Microsoft's ActiveX, COM, DCOM and .NET technologies.

C. The SMS shall allow the configuration of integrated workstations which provides photo imaging, alarm and display monitoring, and digital video review–both recorded and live, alarm and display workstations. These workstations, file server(s) and Door Access Controllers (SAC) shall be connected via the clients' high-speed Ethernet backbone running the TCP/IP protocol. Up to 4 million nodes, i.e., workstations, servers, and SACs can be connected to this backbone.

D. The SMS shall be expandable to include, as a minimum, 256 photo imaging and/or 256 alarm and display or integrated workstations.

E. The alarm monitoring and display workstation shall be able to monitor field hardware devices, such as card readers, controllers, and I/O modules. Administrative tasks, such as assigning security areas, schedules, report generation, displaying color graphic maps, etc., shall be provided from any SMS workstation on the network.

F. The DVMS workstation shall permit viewing of live and recorded video

G. from multiple digital video recorders simultaneously. The DVMS

H. workstation(s) shall also allow users to perform remote configuration of the digital video recorder(s) as well as selected or queued door releases, queued alarmed video.

I. The SMS shall utilize a commercially available, Open Database

J. Connectivity-compliant (ODBC), SQL open architecture relational database with flexible design allowing the integration into other data structures. This database shall handle the storage and retrieval of all card holder records information, images, system maps, reports, and screen designs. The database shall operate in a truly multitasking environment without degradation of system operation and be of a design that will handle the transaction loading placed on the system.

K. The SMS shall allow for SNMP trap and port monitoring by IT software.

1.8.2 System Design

The SMS shall be designed to perform a wide variety of features and functions. These system functions should be categorized into four primary "system components" which shall include:

1. **Access Control -** The SMS's primary purpose shall be to provide access control. The system shall be able to make access granted or denied decisions, define access privileges, and to set schedules and holiday groups. And through the use of application

programming these inputs and outputs shall be capable of being linked at all field controllers for purposes of implementing system-wide control strategies. The system shall support features such as area control, anti-passback, and extended shunt time. The SAC shall be capable of executing all these functions in a stand alone condition, not connected to the network or PC workstations.

2. **Alarm Management -** The SMS shall be used for alarm monitoring. A color graphic application shall allow a user to create or import customized color graphic maps of their facility and to attach alarm icons to those maps. Alarms are to be prioritized. A status window shall provide information about the specific alarm including date and time and location of the alarm. The SMS shall allow unique emergency instructions to be specified for each type of alarm. Output control operations shall be available to lock, unlock, or pulse control points or groups of points as a standard feature. A user shall be able to log comments associated with the alarm and this shall be stored in the database for future review. An image comparison feature shall be provided for use in conjunction with a DVMS technology interface. The SMS shall allow up to four DVMS cameras connected to the digital video recorder workstation(s) to be associated with any alarm device, physical or virtual. Upon activation of an alarm the SMS shall automatically permit an authorized user to query the pre- and post-video that was recorded and associated with the alarm from any of the associated camera(s).

3. **Card Holder Management and Enrollment -** The SMS shall include an employee management system integrated with the access control system. This employee management functionality shall allow the enrollment of card holders into the database, capturing of images, and import/export employee data. The importing function shall support .csv interface to facilitate integration with Windows Active Directory. This functionality shall also allow the user to assign or modify access privileges of a cardholder, assign elevator access, capture ID Badging information. The SMS shall include the ability to capture employee images but a photo ID printer will not be required. The purpose of the employee images will be to allow operators of the system to verify images.

4. **System Administration -** System Administrative tasks such as defining workstation and user permissions, area access, schedules; generation of reports; displaying and interacting with facility/site maps; etc. shall be available at any SMS workstation on the network. System backup and remote diagnostics shall occur at the designated file server that provides the required hardware. Additionally, the SMS System Administrative functions shall allow an operator to monitor, control, and configure those items listed in section 1.2.A from the SMS GUI.

2 PART 2 – PRODUCTS

2.1 Operational Requirements

A. The design of the SMS shall include devices and equipment used to monitor and control access to restricted areas, detect and deny unauthorized entries within specific buildings or areas, annunciate alarms and generate reports. The SMS shall also provide Digital Video Management System (DVMS) integration and allow easy retrieval of recorded video and viewing of live video. Once incorporated with the day-to-day operations of the designated facility, the SMS shall detect and deter unauthorized entry into restricted areas and permit integrated DVMS surveillance to permit viewing of recorded video associated with alarm events. The SMS is to be designed and configured to provide operational flexibility and reliable performance.

B. Functional Responsibilities - CUSTOMER shall have the responsibility for managing and operating the system. It shall be the responsibility of the CUSTOMER to enroll all personnel and capture the associated images. It shall be the responsibility of the SMS contractor to install, configure, program, and train the customer on the SMS system, day-to-day operation of the SMS System to the customers' satisfaction. The SMS contractor and the CUSTOMER will work together to configure the remote connectivity portion of the project.

C. Operational Concept - The SMS shall consist of equipment and devices placed at predetermined locations as depicted on the drawings to ensure that only cardholders who are authorized to enter secured areas through certain doors or gates can do so. This shall be accomplished by means of a computer and electronic devices used in conjunction with door locks, gate systems, over head doors, and card readers.

    1. When an employee is newly hired or is changing job responsibilities, a personnel form shall be available within the SMS application. This employee data screen shall contain, at a minimum, 128 data entry fields of information. The employee data screen shall allow for multiple pages of user information that can be input upon enrollment. Above and beyond the 64 fixed fields there shall also be 64 user-definable fields. These fields shall vary in character length as dictated by the system. Data fields shall be assigned as alphanumeric or numeric.

2.2 SMS Features

A. All SMS applications shall be easy, quick and efficient to use. The system shall combine keyboard and mouse operations with graphical presentations of onscreen information. The Workstation GUI shall have Icon based menus. Each application is to provide consistent user interfaces across all operations of the system. Standard terminology, practical methods of generating help options, and menus are also required. All routine information displayed and requiring input shall be in English language prose. No operation shall require the interpretation of machine code or the use of mnemonics. Remote connectivity to the system shall also be provided through a secured RDP session.

B. Access Control

    1. Access Privileges - All cardholders shall have facility access based on privileges assigned by controlled area, time and date. For example, some badges shall only allow access to the facility on weekdays between 8:00 a.m. and 5:00 p.m., while others allow access on weekends between 1 p.m. to 5 p.m. and so on. These time zones for each day are to be pre-defined by CUSTOMER and shall be able to be modified quickly by authorized employees without vendor intervention. There shall be an unlimited number of user-definable access privileges.

    2. Holidays - The Holidays application shall allow the System Administrator to create holiday schedules that designate individual days as holidays, or special days to cover vacations, maintenance shutdowns, or other events, indefinitely into the future. Holidays or special days can signal that the system shall operate on a schedule different from the normal. Holiday schedules shall be capable of overriding normal schedules.

3. Time/Date - The time and date of the system shall be set by the operating system of the client workstation. Dates for Daylight Savings Time shall automatically take effect.

4. Global Data Exchange and Operating Strategies - The SMS shall provide global data exchange and operating strategies. The system shall allow any input point configured in the system (i.e., door, tamper, duress, etc.) to permit activation of any control output point such as a relay(s) that opens a door and/or sounds an alarm. The logic shall be developed using an application programming language that shall be capable of incorporating other parameters such as date and time; it shall not be limited by a fixed numbers of rules, or the simple linking of inputs to outputs. The global operating strategies feature shall provide the ability to drive any system output or outputs from single or multiple inputs, access events, alarms, etc. Each output point shall be controllable by the system and be configurable individually for the following responses:

    a. Output relays (and groups) shall be capable of responding to:

        i. Input alarms from any I/O module or card reader point in the system, or any combination thereof.

        ii. Access events.

        iii. Date and time parameters.

        iv. Commands from a user.

    b. Output relays (and groups) shall be capable of:

        i. Pulsing for a predetermined duration; duration shall be programmable for each relay individually.

        ii. "Following" any input point from any I/O module, or card reader input in the system (on with alarm, off when clear, or as required).

        iii. Locking On with alarm, requiring user intervention to reset the output relay.

        iv. The system shall permit output relays to be ordered on, off, pulsed or reset back to a default setting.

5. Shunt Time - Shunt Time feature shall be provided to allow users to program, at the door level, a length of time to hold a door open without creating an alarm condition at the monitoring workstation. The shunt time feature shall be usable by any cardholder with an active badge and appropriate access rights. Valid open times shall range from 0-255 seconds. If the door fails to close prior to the expiration of the shunt period, a "door held open" alarm shall occur at the system's monitoring workstation. If the door is closed prior to the expiration of the shunt period, the door position switch shall become active immediately, allowing a "door forced open" alarm to be annunciated in the event of an intrusion.

6. Area Control - The SMS shall provide seven area control features: hard anti-passback, soft anti-passback, timed anti-passback, multiple-man rule, occupancy limit, Area Lockdown and Condition level access, executive privileges, and threat level conditioning. Area control shall be a security method of preventing a person from passing their badge to another person for dual entry into a location utilizing one card. Specifically for this project the Area Lockdown functionality shall be configured in coordination with the client.

    a. Area Lockdown

        i. Area Lockdown shall allow securing of an Area based on any of the following:

        a) User entry via a graphical icon
        b) Automatically triggered based on an alarm or based on a status change of any input to the system.
        c) Utilization of a manual desk mounted panic button/

    A card holder can be given a special privilege that will allow access during a lockdown condition.

7. Manual Control - A user shall have the ability to easily dictate manual control of all output points connected to the system via color graphic maps. Control points are defined as any door strike or any other relay output point of an I/O module. The System Administrator shall have the option to group these outputs to simplify common output command procedures. All system outputs shall be displayed upon command in a list window or graphic map. The list and commands shall be operational without interfering with alarm monitoring operations. If an output is ordered to a setting, and is also on time zone control, the last command shall always override. All manual control commands shall record into the activity log for viewing by any user given proper privileges to do so. Manual control for doors, or any relay output, shall allow the user to disable the door/output (to not accept any cards), unlock the door/output (leaving the door strike unlocked), pulse the door/output open, or reset the door/output to a pre-defined default setting.

8. Arm/Disarm - The user shall have the ability to determine the current status (armed or disarmed) as well as the current state (alarm/normal/fault) of an input point from an input list view at any time. The user shall have a “Status” item in the list view. Both the current status and state shall be reflected by the color of the respective columns in the list view. Arm-Disarm shall be accomplished by a user through a simple click of the mouse on the individual point, a key switch input or automatically via a schedule. Once a user arms an input point, events from the respective area permit the display of alarms at an alarm monitoring workstation from that point forward. All input points shall be grouped for ease of operation into arm-disarm groups. The arm/disarm functionality shall exist if the I/O points are connected to the Access Control System or the IDS system. If connected to the IDS system each I/O point shall be also configured into the SMS system GUI. Any 3rd party IDS monitoring will be provided by others.

9. Alarm Management

    a. General - The software shall be capable of accepting alarms directly from controllers, or generating alarms based on polling of data in controllers and comparing to limits or conditional equations configured through the software. Any alarm (regardless of its origination) shall be integrated into the overall alarm management system and shall appear in all standard alarm reports, be available for user acknowledgment, and have the option for displaying graphics, or reports. Alarm management features shall include:

    1) A minimum of 255-alarm notification levels. Each notification level shall establish a unique set of parameters for controlling alarm display, acknowledgment, keyboard annunciation, alarm printout, and record keeping.

    2) Automatic logging in the database of the alarm message, point name, point value, connected controller, timestamp, username, time of acknowledgement, and time of alarm silence (soft acknowledgement).

    3) Automatic printing of the alarm information or alarm report to an alarm printer or report printer.

4) Sounding of an audible beep or playing an audio (.wav) or displaying a video (.avi) file on alarm initiation or return to normal.

5) Sending an e-mail and/or alphanumeric page to anyone listed in a workstation's e-mail account address list on either the initial occurrence of an alarm and/or if the alarm is repeated because a user has not acknowledged the alarm within a user-configurable timeframe. The ability to utilize e-mail and alphanumeric paging of alarms shall be a standard feature of the software integrated with the operating system's mail application interface (MAPI). No special software interfaces shall be required.

6) Sending a text message to an alphanumeric pager compliant with the TAPI protocol.

7) Individual alarms shall be able to be re-routed to a workstation or workstations at user-specified times and dates. For example, an invalid card read alarm can be configured to be routed to a system administrator workstation during normal working hours (7 a.m.-6 p.m., Mon-Fri) and to a Central Alarming workstation at all other times.

8) An active alarm viewer shall be included which can be customized for each user or user type to hide or display any alarm attributes. As a minimum, the alarm viewer shall display:

   i. Date and time of alarm
   ii. Name of alarm
   iii. Priority of alarm
   iv. Type of alarm
   v. Alarm message
   vi. User text input
   vii. User action drop-down list
   viii. Acknowledged by
   ix. Date and time of acknowledge
   x. Silenced by
   xi. Date and time of silence

9) The font type and color, and background color for each alarm notification level as seen in the active alarm viewer shall be customizable to allow easy identification of certain alarm types or alarm states.

10) The active alarm viewer shall be configured for critical alarms such that a user is required to type in text in an alarm entry field and/or pick from the user action drop-down list. This ensures accountability (audit trail) for the response to critical alarms.

11) The user shall have the ability to Soft Acknowledge (i.e., Silence) or Acknowledge the alarm. Each of these actions shall be logged and date/time stamped.

12) Each alarm shall be configured to be acknowledged under the following:

   i. Acknowledge all of the same alarm type.
   ii. Acknowledge all of the same alarm types until a specified time.

    iii. Acknowledge only highlighted alarm.

13) The user shall have the ability to configure how alarms are removed from the active alarm view based on:
    i. Acknowledged
    ii. Returned to normal
    iii. Acknowledged or returned to normal
    iv. Acknowledged and returned to normal
    v. Acknowledged after returned to normal

14) The user shall have the ability to highlight a specific alarm and select a button to display an associated graphic map, or select a button to display an associated report.

15) When an alarm is acknowledged, the system shall request a User Name, Password and Operator text description to be entered.

16) Other alarms shall be displayed by the system while any alarm is being addressed. If another alarm occurs, the alarm pending counter shall increase by one, the new alarm shall enter into the alarm list box prioritized in an order as defined by the System Administrator.

17) The SMS shall allow journals to be retrieved, viewed, and edited onscreen. Journals shall be saved to tape during tape backups for a permanent record as required by CUSTOMER regulations.

b. Current Status Indication - The active alarm view shall provide a status indicator that displays the current status of alarms and field controllers. Selecting the graphic icon shall provide the user with a detailed list of the groups of devices offering a dynamic list view of the current status of the respective points.

c. Card Holder Record Call-up - The user shall be able to initiate the call-up of a cardholder record. This feature shall be provided at all Alarm and Display Monitoring Workstations to assist the user in determining access rights for an employee who may have forgotten their badge. Utilizing a database search via the input of the cardholder's name, or other key search fields, the SMS shall access the employee's personnel file, containing pertinent information and the employee's image for identification by the user. This operation shall not restrict the operation of monitoring alarms. The SMS system will also provide the ability to send email notifications when an invalid card is used at a card reader.

d. DVMS Video Integration – Pelco - Activation of an alarm point, physical or virtual, shall automatically spawn the alarm video window to allow an authorized user to view the live video associated with the alarm area, as well as the pre- and post-video that had been recorded and associated with the alarm. Up to four cameras may be associated with each alarm point. A user shall also be able to query past video using date/time parameters and alarm device names.

e. DVMS/Image Comparison - The recall of photo images taken by the SMS may be displayed in response to a card read alarm (e.g., access denied out of time zone, no access to area, badge voided, etc.), or any condition for that matter, at any user workstation. This is accomplished by selecting the event desired and displaying the record of the cardholder selected. An interface to the DVMS system shall permit the automatic call-up of a camera located near the card reader in alarm and display the live DVMS image on the workstation, or an adjacent video monitor for user comparison of the images. This shall allow immediate user comparison of the cardholder at the reader and the image on record for the card number. The user shall have the option to pulse the door open for the cardholder from this window. The DVMS image shall be printable from the image comparison screen, if the monitor is equipped with a thermal video printer or a laser printer.

   f. Automatic User Logoff - The system shall automatically log the user out of the application after a specified period of inactivity. The user shall have to log back into the system to handle an alarm. This feature shall be configurable on a user by user basis by the system administrator.

   g. Scheduling - Time of day schedules shall be in a calendar style and shall be programmable up to 10 years in advance. Each standard day of the week and user-defined day types shall be able to be associated with a color so that when the schedule is viewed it is very easy, at-a-glance, to determine the schedule for a particular day even from the yearly view. To change the schedule for a particular day, a user shall simply click on the day and then click on the day type. Each schedule shall appear on the screen viewable as an entire year, month, week, and day. A simple mouse click shall allow switching between views. It shall also be possible to scroll from one month to the next and view or alter any of the schedule times. Schedules shall be assigned to specific controllers and stored in their local RAM memory. Any changes made at a workstation shall be automatically updated to the corresponding schedule in the controller. Schedules shall be downloaded to the respective controller on a weekly basis.

10. Card Holder Management and Enrollment - The SMS shall incorporate into a single, integrated system the latest in imaging technology and identification management. The SMS shall generate and store up to four million personnel records, and monitor badge/credential use throughout the facility. These credentials shall be based on data and images that are input and captured at the time of enrollment and fabricated at any of the SMS photo imaging workstations.

11. Create and Maintain Personnel Database - The user shall be able to create personnel records either through the use of templates (as described in System Administration section), or direct input into the personnel record. Each personnel record shall allow for easy navigation through the fields using either the “tab” key or a mouse. The user shall have the ability from the personnel record to easily:

    a. Enable or disable the cards.

    b. Define expiration date.

    c. Define the acceptable card type.

    d. Define the card number, site code and PIN.

    e. Mark the card as lost.

    f. Issue temporary or restore permanent card.

    g. Display the employee photo image.

    h. Have the ability create or edit the image.
    i. Create, edit, or delete the cardholder’s access privileges and additional personnel attributes.

12. The selection of card type shall be chosen from a drop-down list that shall include ABA formats, Wiegand formats, and custom Wiegand format to allow use of a Customer’s existing cards that may be of a format not standard within the SMS.The expiration date shall be determined by date and time of day carried out to the nearest second. The user shall be able to mark the card as lost by selecting that control button. This shall disable the card and create a stored record with the associated card number and cardholder. A new record shall automatically be created allowing the user to only have to add the new card number. In the event an attempted use of the card occurs, an invalid card event shall be logged and an associated alarm can be generated to an operator workstation. The user shall be able to issue a temporary card by selecting that control button. This action shall temporarily store the existing card number and allow the user to then simply enter into the record the temporary card number. Upon return of the temporary card, the user shall select the reissue permanent card control button, which shall automatically restore the original card number.

13. Assigning Access Privileges - After a badge is created it shall be possible to assign access privileges to the personnel record. For convenience, the System Administrator shall be able to define default templates for given personnel types. If a user has proper authorization, access privileges can be overwritten. When an individual’s access privileges are modified, that change shall automatically be propagated to all required controllers immediately upon completion of the change. Record changes of access privileges shall affect only the modified record, and shall not require a download of the entire cardholder database. Using personnel record configuration templates, the SMS System Administrator shall be capable of attaching previously defined privileges attached to the templates to new personnel requiring similar privileges. It shall be possible for the System Administrator to individually access the newly created personnel record to modify the privileges in the event the person does not exactly comply with the template.

14. Badge Creation
    a. Image Capture - Each SMS photo imaging workstation shall include all equipment required to capture a high quality portrait image, with flash lighting and a high quality RGB digital video camera. The photo imaging workstation shall allow the camera user to view a live video image of the subject on the screen. The user shall view the subject in an upright position as they are captured. While capturing subjects, the user shall have the option of capturing a new image of any subject without affecting the subject’s record. The photo imaging workstation shall provide a digitizer color control window in order to adjust the contrast and brightness of images. For convenience, default settings shall be provided. The system shall provide the ability to move via mouse a “capture window” over any portion of the live image displayed on the monitor and store only the image information within the outline of the window. The SMS shall include the ability, upon command, to preview, online and in full color, the badge as it will appear when printed. This preview mode shall require less than 10 seconds to create a complete example of the badge online. SMS image capture, storage, and hardware compression techniques shall be in compliance with the ANSI X3L2.8 standard or JPEG.
    b. Pre-defined Badge Formats - The badge format, including background color, layout, location of photo image, applicable graphics or company logos, text, etc., shall be

completely and automatically determined by the system based on employee record information. Where choices are available to the user, choices are to be made via pre-defined list boxes to avoid user errors in spelling and badge assignment errors.

c. Search Records - The SMS shall allow the user to search for records and images using search criteria on any field(s) in the database. The user shall be able to enter the search criteria for one or a combination of fields

2.3 System Administration

A. General

The workstation software shall use a familiar Windows Explorer-style interface for a user or programmer to view and/or edit any object (controller, point, alarm, report, schedule, etc.) in the entire system. In addition, this interface shall present a "network map" of all controllers and their associated points, programs, graphics, alarms, and reports in an easy-to-understand structure. The configuration interface shall also include support for template objects. These template objects shall be used as building blocks for the creation of the SMS database. The types of template objects supported shall include all data point types (input, output, string variables, etc.), personnel records, doors, alarm algorithms, alarm notification objects, reports, graphics displays, schedules, and programs. Groups of template object types shall be able to be set up as template subsystems and systems. The template system shall prompt for data entry if necessary. The template system shall maintain a link to all "child" objects created by each template. If a user wishes to make a change to a template object, the software shall ask the user if he/she wants to update all of child objects with the change. This template system shall facilitate configuration and programming consistency and afford the user a fast and simple method to make global changes to the SMS. All object names shall be alphanumeric and use Windows-type long filename conventions. The SMS shall allow all objects (door, personnel record, alarm, etc.) to be created with a unique 64-character name to provide the user with a fully descriptive object identifier. The system shall automatically create up to a 16-character alias from the object name to simplify the object's use in reports, applications programs, and alarms, for example.

B. Workstation and Password Privileges

The software shall be designed so that each user of the software can have a unique username and password. This username/password combination shall be linked to a set of capabilities within the software, set by, and only editable by, a system administrator. These sets of capabilities shall range from view only, acknowledge alarms, enable/disable, change values, program, and administrate. The system shall allow the above capabilities to be applied independently to each class of object. The system shall allow an unlimited number of users to be configured per workstation. The SMS shall allow the system administrator to configure each workstation with those functions that may be performed at that workstation. Individual user passwords shall also further restrict user functions and shall be specific to each user. Specific user restrictions shall include:

1. Access to screens or functions (e.g., alarm monitoring, badge issue)
2. Specific tasks allowed (e.g., modify data, view only)
3. Alarm monitoring functions (e.g., clear alarms, output control,
4. traces, reports, arm-disarm)

If a user is denied access to specific functions, those functions shall dimmed on the user's workstations or the status bar shall indicate "access denied" while that user password is logged in. A User shall be able to change their own password at any time. Passwords shall automatically expire after a defined number of days between 7 and 180 as set by the System Administrator. A minimum password length shall be settable by the administrator to be between 1 and 16 characters. The SMS shall support individual password restrictions for each user. The SMS shall offer the option of using a Windows user account to access the system.

C. Create and Maintain Door Objects

Door objects shall be created either through the use of templates (as described in section 2.2.4.1) or by direct input by the user. The door object editor shall be organized with tabs for easy navigation through the attribute fields. From the door record the user shall be able to:

1. Document a description of the door
2. View and/or change the door's current state from unlocked to locked and vice-versa
3. View the state of the door switch
4. Enable or disable the door state
5. Specify up to four acceptable site codes
6. Choose between Wiegand or ABA card type and select the appropriate bit format
7. Associate door hardware wiring to the appropriate input/output channels
8. Attach specific door unlock and door lock schedules
9. Define readers and attach associated controlled areas
10. View a list of the last 25 events associated with the door

D. User Activity Logging

The SMS shall provide full user activity tracking. The activity log shall be comprehensive, recording the date and time of the activity, the workstation where the activity was performed, and the user that performed the activity. The SMS shall record changes to the database made by any user. Users shall be prompted to enter a user name, password, and explanatory text before any change or command is made to the system. Changes shall include point control changes, point edits, commands from a graphic panel, schedule changes, etc. This additional information is saved in the activity log for future reporting. Users shall be able to maintain their own passwords and the system shall automatically prompt the user to change their password on periodic basis. SMS shall log over 200 separate functions, including:

1. User log-in and user log-out.
2. Additions, changes, and deletions to cardholder management.
3. Temporary pass add and delete.
4. Other critical database functions.

SMS shall log changes made to the access control configurations:

1. Changes to access privileges.
2. Holidays.
3. Time zone changes.
4. Other critical items.

SMS shall log all activity including alarms, alarms acknowledged, cleared, output control activity, trace, and other functions. The SMS shall log a minimum of 1,000,000 events before the system history overwrites the oldest data. The SMS shall provide a user activity report to query this information available in the SMS activity log. The report shall be sorted by workstation, user, date and time, or other selection criteria. On those occasions when historical data shall be needed, the

E. Screen Format Design

The SMS shall allow a System Administrator to customize the employee record containing employee data. Additional data fields shall be definable in the database. Eighty user-defined data fields shall be available.

F. Integrated Development Environment

Each Alarm, Display, and Integrated workstation shall be equipped with an integrated development environment (IDE) to allow users the ability to write, edit, and de-bug the application programs resident in the Intelligent Door Access Controller (SAC). The IDE shall allow the display of multiple windows of application programs so users can quickly and easily “copy and paste” programming code using simple mouse clicks from one to another. The IDE shall also provide a tool set to allow users to quickly access libraries of commonly used object names, functions, values, and application programming keywords. Use of an IDE wizard shall permit use of pre-written application programs and creation of new programs that prompt for key values and create the program code automatically.

G. Reports

The SMS shall have the capability to provide as a minimum, the following standard reports:

1. User Activity Log
2. Alarm History Log
3. Door Status Report
4. Alarm Point Status Report
5. Controller Status Report
6. Workstation Status Report
7. Event History Log
8. Invalid Attempt Log
9. Valid Access Log
10. All Personnel Report
11. Disabled Personnel Report
12. Personnel by Department Report
13. Personnel by Area Privileges Report
14. Lost Card Report
15. Input/Output Status Report
16. Schedules Report
17. Termination Report

18. Badge Pending Expiration Report
19. Cards Not Used in x days (Deadbeat Report)
20. All Doors Report
21. All Events Sorted by Door
22. All Events Sorted by Person

H. System Backup

A mandatory requirement, the SMS shall provide backup and restore programs utilizing the multi-tasking capabilities of the SMS which run concurrent with any other application of the system and in no way inhibit other use of the terminal. Database backup shall occur dynamically while other alarm monitoring, photo imaging, and/or access control applications remain active. The number of active events to be stored shall be user-definable. If the event log is filled to capacity before an archive backup is done, the system shall start to overwrite the oldest events to make room for the newer events (FIFO). The following functions are required for the database backup procedure of the system application:

1. Archive Information - This function shall indicate how many days worth of event history is maintained on the system.
2. Warnings - The SMS shall provide a configurable warning to allow a System Administrator to enable and define automatic system warnings. These warnings are to be sent to all currently active alarm monitoring workstations to notify the users when the event log is starting to get full.
3. Capacity - The event queue storage capacity shall be displayed as a number up to eight digits long that shall specify the number of event records that can be stored on the system. This number shall be determined by the size of the fixed disk drive installed and is to be generated by the system's database.

I. Color Graphic Map Configuration - The system shall have the ability to draw, edit, and copy site color graphic maps using any third-party system software. At a minimum the map configuration software shall import map drawings from the following formats:

1. JPEG (.jpg)
2. Windows Bitmap (.bmp)

These architectural-type maps shall allow the detailed layout of an entire structure, part of a structure, a floor or department within a building, or layout the periphery of a facility. Overview maps of an entire facility or campus shall be viewable as requested, or a specific entry point of a facility can be accessed via graphic panel objects that shall be able to be configured with multiple "tabbed" pages allowing a user to quickly view individual graphics of equipment, which make up a subsystem or system. Once a map has been drawn, the user shall have the ability to place system level icons of card readers and input points in the appropriate area to indicate their respective location on the map. This is to be accomplished by simply dragging the icon with the mouse to the appropriate location on the map. The SMS shall permit use a full library of these controls including knobs, dials, gauges, switches, peripheral devices such as lights, motion detectors, doors, etc., shall be provided as part of the SMS software. The system shall allow various maps to be associated with each area to provide for the creation of a hierarchy of maps. The SMS shall support graphic maps having a minimum resolution of 1024 X 768 pixels.

2.4 SMS Server/Workstation Requirements

A. The SMS shall be a fully integrated solution operating on a primary database fileserver with capability to have complete redundancy being performed by a hot redundant secondary fileserver. Each SMS workstation shall communicate across an enterprise class TCP/IP network regardless of network connection medium (copper, wireless, SCADA, etc). The SMS system shall allow the centralized database to operate either on a single workstation or remotely through a separate database engine server. If desired by the client the SMS system shall be deployed to operate in a virtual environment with certain system functions being performed in existing virtual operating environments.

The client software on a multi-workstation system shall access the file server database via an Ethernet TCP/IP network. Workstation(s) and file server shall be capable of residing directly on the Customer's Ethernet TCP/IP LAN/WAN with no required gateways.

Workstation(s) and file server shall be capable of using standard, commercially available, off-the-shelf Ethernet infrastructure components such as routers and hubs. With this design the CUSTOMER may utilize the investment of an existing or new enterprise network or structured cabling system. This also allows the option of the maintenance of the LAN/WAN to be performed by the Customer's Information Systems Department as all devices utilize standard TCP/IP components.

The system shall allow future expansion to include additional defined workstations without losing functionality. For multi-workstation systems, a minimum of 1,000 workstations shall be allowed on the Ethernet network along with the central file server. In this client/server configuration, any changes or additions made from one workstation shall automatically appear on all other workstations without the requirement for manual copying of files.

Multi-workstation systems with no central database will not be acceptable.

In addition to the above LAN/WAN architecture support, the same workstation software (front-end) shall be capable of managing remote systems via standard dial-up phone lines as a standard component of the software. Front-end "add-on" software modules to perform remote site communication will not be allowed. System administration operations shall be available from any workstation on the system. System Administrator functions include the creation of customer-specific facility map configurations, alarm response instructions, access privileges, schedules, holidays, field hardware groups, arm-disarm groups, area control, output groups, application programs, and all required system configurations. The SMS shall include a network file server with integrated database.

B. In addition to the computer equipment listed above, the following minimum hardware requirements:

1. Software shall include MICROSOFT SQL Server and Microsoft Workstation Software(s) operating systems.
2. Server software will support both 32 bit and 64 bit environments.
3. Workstation software will support both 32 bit and 64 bit environments.
4. License agreement for all applicable software licenses to support the deployment.
5. RDP software application.

6. SMS Server/Workstation shall be provided by the client.

C. Computer Hardware - Unless otherwise stated, computer equipment needed for each workstation consists of the following minimum requirements:

1. Latest Pentium processor
2. 1 GB of RAM
3. 10/100 Ethernet NIC
4. 180 GB hard drive
5. CD-RW drive
6. Quad monitor cards capable of supporting streaming video from multiple sources at the same time.
7. SVGA compatible, 20" LCD monitor.
8. Full-function keyboard & mouse
9. Audio sound card and speakers
10. License agreement for all applicable software

D. Alarm Monitoring and Display Workstation - The alarm monitoring workstation shall be provided with full imaging display capability and shall be configured to perform alarm monitoring operations. The following major alarm Monitoring tasks shall be included: graphical alarm monitoring, acknowledging alarms, performing traces, output control functions, and badge record lookup. In addition, the alarm monitoring workstation shall also be utilized as an administration workstation as required. The alarm monitoring and display workstation shall be the main workstation for providing the alarm monitoring and access control features described in this specification.

2.5 SMS Field Hardware Devices

1. Overview - The SMS shall be equipped with the field hardware required to receive alarms, administer all access granted/denied decisions, provide interface capability to third-party systems, and implement global operation strategies. Depending upon the configuration, the SMS field hardware shall be able to include any or all of the following features:

1. Real-time Clock (RTC)

A battery-backed RTC shall provide the following information: time, day, month, year, and day-of-week. In normal operation the system clock will be based on the frequency of the AC power. The system shall automatically correct for daylight-saving time and leap years. The system shall provide means to synchronize the time between all controllers and workstations on the network.

2. Automatic Restart after Power Failure

Upon restoration of power, all controllers shall automatically and without human intervention: update all monitored functions; resume operation based on current, synchronized time and status, and implement special start-up strategies as required.

3. Indicator Lamps

As a minimum, all controllers shall have LED indication of Power Status, CPU/Activity status, Comm status, and Error status.

4. Packaging

The Door Access Controller (SAC) and I/O modules shall be cased in a sleek, lightweight plastic housing. The mechanical design will incorporate built-in cable management troughs for wiring runs.

B. Door Access Controller – Andover Continuum ACX Series or NCII Series - The Door Access Controller (SAC) shall provide overall system coordination, accept control programs, perform automated control functions and security management, and perform all necessary mathematical functions. It shall also be possible to permit multi-user operation from workstations and laptop service tools connected either locally or globally. The SAC communication will be based around the Customer's existing Ethernet network at 10/100Mbps. A separate, dedicated, security network shall not be required. The SAC shall be a native TCP/IP device and shall not require use of terminal servers or other devices to allow direct Ethernet connectivity. Use of PCs that serve as Ethernet gateways to the field controllers shall also not be acceptable. The interface link to other systems shall take place at the SAC and not at a central computer, so that in the event of failure of the controller, the rest of the system shall continue to function correctly.

1. SACs shall be microprocessor-based, multi-tasking, multi-user, and use real-time, digital control processors. Each control panel shall consist of modular hardware including power supply, CPU board, and various input/output modules. A sufficient number of SACs shall be supplied to fully meet the requirements of this specification and the attached point list.
2. The SAC shall be equipped with an application programming environment to allow users to create custom applications. All application programs are to be developed using an easy-to-use plain English-oriented programming language inclusive of a complete set of Boolean logical expressions. Use of high level programming languages such as C or C++, or system manufacturer defined "canned" application programs will not be permitted. Application programs shall be used to enhance the functionality of the SMS by permitting custom control strategies and third-party user interfaces to be implemented. All programs shall be self-documenting by allowing the users to place comments anywhere within the body of the program. All global data shall be capable of being referenced at any SAC or I/O module and used in application specific programs to control an output, or multiple outputs at that controller. Use of simple matrices to allow linking of inputs to outputs to meet this intent is not acceptable.
3. Memory - A minimum of 128MB of RAM with math coprocessor shall provided for the SACs. In addition, each controller shall contain a minimum of 32MB of Flash memory for the system firmware and application configuration data. Firmware shall be updated online. Use of EPROM-based firmware requiring chip change-out to perform upgrades is not acceptable.
4. Card Readers Inputs - The card reader inputs shall have a dedicated processor to support current and future devices for advanced applications. Each input can be connected to a card reader, dedicated keypad or reader/keypad combination. The SAC shall accept standard formats (such as Weigand, ABA, HID Corporate 1000, CardKey) as well as custom formats (such as Custom Weigand, Custom ABA). The SAC shall be capable of supporting 260 bit encrypted data messages from the reader.
5. Inputs/Outputs
    i. Input

The input section of the access I/O modules shall provide a minimum of one card reader channel and one keypad channel. It shall be possible to expand the number of card readers by simply adding I/O modules to the communications network. In addition, there shall be three supervised inputson the base controller for request-to-exit devices, door status devices, and general supervised input monitoring. The card reader inputs shall accept Wiegand or Magnetic Stripe style readers. Up to 64 bits per card formats shall be supported for Wiegand applications and up to 255 bits per card formats shall be supported in ABA applications. Each supervised input shall be able to distinguish among normal operation, a short, open circuit, or a fault. Inputs shall be able to use double resistor-based supervised circuits. A normally open momentary switch shall be used for external tamper detection. This switch shall detect whenever the cabinet of the access control module has been opened. The access control module shall support Wiegand output or ABA output keypads. The keypad data shall be superimposed onto the Wiegand or ABA data lines.

ii. Outputs

Output types shall be digital for control of doors. In addition to the door output, the control module shall contain one auxiliary output for ON/OFF control of annunciators, lights, etc. Outputs shall be available with built-in override switches. The digital outputs shall be rated for 24 VAC/DC operation at 5 amps minimum. Each output shall have a corresponding LED for visual indication of its state. A board-mounted three-position switch shall be provided for each output allowing local overrides. The position of the switch shall be detectable in software and available for alarm annunciation. If override switches are not provided on board, external switches shall be provided and wired to include feedback and alarming of the switch position and shall be mounted in a locked enclosure.

C. Intrusion Detection and Peripheral Devices

1. Description - Intrusion detection and peripheral devices shall provide inputs and outputs to monitor and control non-reader-based system points, such as door contacts, motion sensors and panic buttons. All intrusion devices will be integrated into the SMS system so each individual point is monitored, controlled, and alarmed from the SMS GUI. It shall be possible to logically link any intrusion device to any other SMS device for full integration and alarming. UL 1076 requirements will apply to the SMS controllers.

    a. Input/Output SMS Points

        i. Inputs

        Each supervised input circuit shall be able to distinguish among normal operation, a short, open circuit, or a fault. In addition, these same inputs can be configured for analog operation to monitor temperatures, humidity, or other transducers outputting industry standard signals of 0 - 5 VDC and 4 - 20 mA.

        ii. Outputs

        The output type shall be digital using Form-C relays capable of switching 24 VAC/DC at 5 Amp. Each output shall have a corresponding LED for visual indication of its state. Outputs shall be available with built-in override switches. A board-mounted switch shall be provided for each output allowing local overrides. The position of the switch shall be detectable in software and available for alarm annunciation. If override switches are not provided on board, external switches shall be provided and wired to include feedback and alarming of the switch position, and shall be mounted in a locked enclosure.

b. Door Contacts – 1078

CUSTOMER requires the SMS system to utilize flush mounted door contacts on each perimeter door, access control door, and time-locked door.

c. Overhead Door Contacts – 2202A

CUSTOMER requires the SMS system to utilize surface mounted door contacts on all overhead doors located on the perimeter of the building.

d. Interior Motion Detectors – Bosch DS-937X Series

CUSTOMER requires the SMS system to include interior motion detectors in key areas as shown on the drawings. Motion detectors shall be ceiling mounted to allow 360 degree coverage.

e. Duress Buttons – HUBM

CUSTOMER requires the SMS system to include duress buttons in key areas as shown on the drawings.

f. Field Hardware Power Supplies – Altronix AX-600 Series with ACM-8.

Power Supplies for field hardware shall be compatible with the SMS equipment installed. Power supplies shall be regulated, linear, and isolated versions for the field controllers and other equipment. All power supplies shall be housed in tampered, locked enclosures. All low voltage power supplies needed to support the access control panels are to be provided and installed by the SMS contractor. Only power supplies for the electrified locking hardware will be provided and installed by the division 8 contractor.

g. Intrusion Panel Dialer (IPD) – Bosch 9412 Series with D1255

The system will be installed with the ability for a central station dial out in the event of an alarm condition. Communications will be provided through a UL listed communications device that is incorporated into an alarm panel that will be integrated into the SMS system. The integration will provide the following functionality (at a minimum):

i. Arming/Disarming of the IPD from the SMS application.

ii. Arming/Disarming of individual zones from the SMS application.

iii. Monitoring of communication lines from the SMS application.

iv. Point ID alarming

D. Card Readers and Biometric Readers

The SMS system shall utilize a uniformed deployment for all reader technologies unless the projects drawings specifically call out variations on the reader technologies. Any variations will be depicted in the SMS systems symbol set or on the individual security drawings. If the CUSTOMER elects to deploy various reader technologies throughout the SMS system it will be the SMS contractors’ responsibility to ensure they operate and integrate with the SMS system as a single system. The SMS contractor will be responsible for removing the 3 existing access card readers from the existing facility.

1. Multitech Card Readers – HID RP40

   If the CUSTOMER requires the SMS to use Smart Card Readers the SMS contractor shall deploy these readers for all reader locations. This product line offers a variety of readers to match CUSTOMER needs. Each reader shall offer a low profile, rugged, weatherized polycarbonate sealed enclosure with multi-color LEDs and a sounder for access granted and denied indications. Each shall be mountable indoor or outdoor. Readers should be capable of reading the existing access card used by the customer.

2.6 Credentials

A. General

The SMS shall utilize card products designed specifically for security applications. Unless specified differently the SMS system shall utilize RF technology for the credentials. Credentials shall be managed from a single and integrated card management module included in the base SMS system. The credential management system will use the existing access cards currently used by the customer.

2.7 Communication Ports

A. Security Access Controller (SAC) - Each SAC shall provide a powerful multi-user solution for network communications and information management across a high speed Ethernet with data transfer rates up to 100 MB.

B. Networking - Each SAC shall be able to exchange information with other SACs over the high speed LAN. The network structure shall be transparent such that each controller may store and reference all global variables available in the network for use in the SAC's calculations or programs. Each SAC shall also have access to any of the readers, card records, inputs, outputs, and calculated variables contained in I/O modules that are connected to it.

C. Power Supply - SACs shall operate on a 24 VAC 50/60 Hz power or a 12-28 VDC auto-sensing power supply.

D. Battery Backup - Each SAC shall have long term memory battery backup providing at least 7 days of memory retention and Flash memory for unlimited application retention. In the event of a flash restoration after 7 days of power outage, the SAC shall automatically request a download of card holder privileges from the workstation.

2.8 SMS Integration

A. It is the intent of this specification to describe and define a fully integrated SMS system to be deployed as a part of this project.

B. For the purpose of this specification a fully integrated SMS system shall be defined as a system that:

1. Allows a single seat of control from the SMS system of multiple related platforms including:
   a) CCTV Systems
   b) DVMS Systems
   c) Intrusion Detection Systems
   d) Over Head Door Control

2. The interface to the DVMS system shall be configured so that DVMS images displayed on monitors and SMS
    a) Switch displayed images of each camera on the workstations
    b) Pan, tilt, and zoom of individual cameras

3 PART 3 - EXECUTION

3.1 Project Management

A. Upon receipt of a purchase order, The Contractor shall assign the project to a specific project manager. Project managers are selected for their skills and experience in organizing complex, multifaceted projects. This will assure effective planning and communication among the numerous people whose efforts are

B. The project manager shall provide the following services:
    1. Written and agreed project plans detailing the successful installation and acceptance of the system within specified time frames.
    2. Coordination and scheduling of all contractor deliverables through project completion including:
    3. Hardware and software configurations.
    4. Installation of equipment.
    5. User training.
    6. Documentation and specific project related requirements.
    7. Provide services or consultation for:
        a) Site preparation.
        b) Credential design.
        c) Screen layout design, formats.
        d) Database design/configuration.
        e) Data input options.
        f) System Administration.
    8. Primary point of CUSTOMER contact for all project communication from receipt of order through final system acceptance.
    9. Preparation of clearly defined project-specific system acceptance criteria.
    10. Appropriate status reporting, attendance at all project meetings.
    11. Formal commissioning of specific project documentation and as-built drawings to the CUSTOMER system administrator and maintenance contractor.
    12. Preparation of agreement for contractor continuing maintenance and schedule.

3.2 Installation

A. Installation of the SMS shall include the appropriate equipment and shall be performed by the electrical contractor assigned to the project by the general contractor. The SMS contractor will be responsible for ensuring the terminations and cabling provided and installed by the electrical contractor are viable for the SMS system.

B. The installation shall include the following:

1. Site planning and system configuration of field hardware and SMS.
2. Complete hardware setup of all system Workstations and peripherals.
3. Complete configuration of all system Workstations, peripherals and installation of field hardware.
4. Setup of specific network software configuration requirements.
5. Badge Design and Screen Format installation and verification.
6. Complete system diagnostics verification.
7. Complete system operation verification.
8. Problem reporting and tracking.
9. Project-specific installation log.
10. Completion of specific customer acceptance test plans. Formal delivery of the specific project installation documentation to Maintenance Service Organization.

3.3 Implementation

Required planning and coordination of numerous elements and deliverables during the installation and commissioning phases shall be handled professionally and within a specified schedule.

3.4 Field Quality Control

A. Quality Assurance

Source Limitations: To the fullest extent possible, provide products of the same kind, from a single source, and from the same manufacturer. Descriptive Specification Requirements: Where specifications describe a product of assembly, listing exact characteristics required, with to without use of a brand or trade name, provide a product or assembly that provides the characteristics or otherwise complies with contract requirements. Performance Specification Requirements: Where specifications

require compliance with performance requirements, provide products that comply with these requirements, and are recommended by the manufacturer for the application indicated. General overall performance of a product is implied where the product is specified for a specific application.

B. Installation of Products

Comply with manufacturer's instructions and recommendations for installation of product in the applications indicated. Anchor products securely in place, accurately located and aligned with other work. The Contractor is responsible to remedy defects due to faulty workmanship and materials that appear within 1 year from the date of acceptance in accordance with the General Conditions, unless Specifications sections specify a different duration.

3.5 System Acceptance Test

A. Phased Testing

A phased acceptance test and performance demonstration program shall be developed and documented by The Contractor under the direction of the SMS Systems Engineer. These requirements shall apply to all system components and software, including, but not limited to all system computers, field controllers, card reader devices, photo imaging system peripherals, DVMS cameras and equipment, and interface capability. The Contractor shall perform the tests and document the results under the supervision and witnessing of the SMS Systems Engineer. Operational scenarios shall be developed and used by The Contractor to simulate the actual use of the system in the normal environment of the CUSTOMER facility. The SMS Systems Engineer reserves the right to modify The Contractor's plan or develop new operational test and evaluation procedures to effectively document system operations.

B. The Contractor shall perform contract field performance verification, and endurance testing and make adjustments of the completed security system when permitted. The Contractor shall provide all personnel, equipment, instrumentation, and supplies necessary to perform all testing.

C. The City of Austin will witness all testing and system adjustments during testing. Written permission shall be obtained from the City of Austin before proceeding with the next phase of testing. Original copies of all data produced during performance verification and endurance testing shall be turned over to the City of Austin at the conclusion of each phase of testing and prior to City of Austin approval of the test.

D. Test Procedures and Reports: The test procedures shall explain in detail, step-by-step actions and expected results demonstrating compliance with the requirements of the specification. The test reports shall be used to document results of the tests. The reports shall be delivered to the City of Austin within seven (7) calendar days after completion of each test.

E. The inspection and test will be conducted by a factory-certified Contractor representative and witnessed by a City of Austin Representative. The results of the inspection will be officially recorded by a designated City of Austin Representative and maintained on file by the City of Austin (RE), until completion of the entire project. The results will be compared to the Acceptance Test results.

3.6 Contractor's Field Testing (CFT)

A. The Contractor shall calibrate and test all equipment, verify DTM operation, place the integrated system in service, and test the integrated system. Ground rods (if installed by this Contractor within the base of camera poles) shall be tested as specified in IEEE STD 142. The Contractor shall test all security systems and equipment, and the Contractor shall provide the City of Austin with a written listing of all equipment and software indicating all equipment and components have been tested and passed. The Contractor shall deliver a written report to the City of Austin stating the installed complete system has been calibrated, tested, and is ready to begin performance acceptance testing; describing the results of the functional tests, diagnostics, and calibrations; and the report shall also include a copy of the approved acceptance test procedure.

Performance verification testing shall not take place until written notice by Contractor is received certifying that a contractors field test was successful.

3.7 Acceptance Testing

A. Performance Verification Test (PVT)

1. Following the Contractor's Field Testing (CFT), the system shall be tested in the presence of a City of Austin Representative (s), and a representative(s) of the Contractor. The test shall verify that the total system meets all the requirements of this specification.
2. The Contractor shall demonstrate the completed security system complies with the contract requirements. Using approved test procedures, all physical and functional requirements of the project shall be demonstrated and shown. The PVT will be stopped when more than (2) technical deficiencies are found requiring correction. If the acceptance test is aborted, the re-test will commence from the beginning with a re-test of components previously tested and accepted.
3. Punch List - Contractor shall record an inspection punch list noting all system deficiencies. The Contractor shall prepare an inspection punch list format for City of Austins approval. The punch list shall include a listing of punch list items, punch list item location, description of item problem, date noted, date corrected, and details of how item was corrected.
4. Partial PVT - At the discretion of City of Austin, the Performance Verification Test may be performed in part should a 100% compliant CFT be performed. In the event that a partial PVT will be performed instead of a complete PVT; the partial PVT shall be performed by testing 10% of the system. The Contractor shall perform a test of each procedure on select devices or equipment.
5. Submittals - Upon successful completion of the PVT test, the Contractor shall deliver test reports and other documentation, as specified, to the City of Austin prior to commencing the endurance test. Additional submittals of the Acceptance Test shall include:
    a. System Inventory
    b. All Device equipment
    c. All Software & associated license documents/keys
    d. All Logon and Passwords
    e. All Cabling System Matrices
    f. All Cable Testing Documents
    g. All System and Cabinet Keys

B. Run Test

The run test is intended to provide proof that the installed security system will perform under actual operational conditions over time as designed. The run test shall be conducted in phases as specified below. The Run Test shall be started when the performance verification test is satisfactorily completed, training as specified has been completed, and correction of all outstanding deficiencies has been satisfactorily completed. City of Austin will operate the system during operating hours dictated by the intent of the system for run testing. The City of Austin will maintain a log of all system deficiencies. The City of Austin may terminate testing at any time the system fails to perform as specified. Upon termination of testing, the Contractor shall commence an assessment period as described for Phase II (Assessment) testing below. During the last day of the test, the Contractor shall verify the appropriate operation of the system. Upon successful completion of the endurance test, the Contractor shall deliver test reports and other documentation as specified to the City of Austin prior to acceptance of the system.

1. Phase I (Run Testing): The test shall be conducted (24) hours per day for (7) consecutive calendar days (unless otherwise specified), and the system shall operate as specified. The Contractor shall make no repairs during this phase of testing unless authorized in writing by the City of Austin. If the system experiences no failures, the Contractor may proceed directly to Phase III testing upon approval from the City of Austin.
2. Phase II (Assessment):
    a. After the conclusion of Phase I, the Contractor shall identify all failures, determine causes of all failures, repair all failures, and deliver a written report to the City of Austin. The report shall explain in detail the nature of each failure, corrective action taken, results of tests performed, and recommend the point at which testing should be resumed.
    b. After delivering the written report, the Contractor shall convene a test review meeting at the job site to present the results and recommendations to the City of Austin. The meeting shall not be scheduled earlier than five (5) business days after the City of Austin receives the report. As part of this test review meeting, the Contractor shall demonstrate all failures have been corrected by performing appropriate portions of the performance verification test. Based on the Contractor’s report and the test review meeting, the City of Austin will provide a written determine of either the restart date or require Phase I be repeated.
3. Phase III (Run Testing): The test shall be conducted (24) hours per day for and additional (7) consecutive calendar days, including holidays, and the system shall operate as specified. The Contractor shall make no repairs during this phase of testing unless authorized in writing by the City of Austin.
4. Phase IV (Assessment):
    a. After the conclusion of Phase III, the Contractor shall identify all failures, determine causes of all failures, repair all failures, and deliver a written report to the City of Austin. The report shall explain in detail the nature of each failure, corrective action taken, results of tests performed, and recommend the point at which testing should be resumed.
    b. After delivering the written report, the Contractor shall demonstrate that all failures have been corrected by repeating appropriate portions for the performance verification test. Based on the Contractor’s report and the demonstration, the City of Austin will determine if Phase III testing needs to be repeated. After the conclusion of any re-testing which the City of Austin may require, the Phase IV assessment shall be repeated as if Phase III had just been completed.

C. Exclusions

1. The Contractor will not be held responsible for failures in system performance resulting from the following:
    a. An outage of the main power in excess of the capability of any backup power source provided the automatic initiation of all backup sources was accomplished and that automatic shutdown and restart of the PACS performed as specified.
    b. Failure of an Owner furnished equipment or communications link, provided the failure was not due to Contractor furnished equipment, installation, or software.
    c. Failure of existing Owner owned equipment, provided the failure was not due to Contractor furnished equipment, installation, or software.
    d. Failure of Owner to provide necessary personnel to Contractor for scheduled activities.

3.8 System Documentation

A. Complete documentation shall be provided with the system. The documentation shall completely describe all operations, each program, data sets, the hardware, and peripherals. All updates, addendum and adjustments to the documentation shall be provided at no additional charge, in the same quantities as originally required. Each division shall define the initial quantities.

1) System Administrator Manual - Overview and step-by-step guide and instructions detailing all System Administrator responsibilities and authority.
2) User Manual - Step-by-step guide and instructions detailing all system user functions and responsibilities.
3) Photo Imaging Users Manual - Step-by-step guide and instructions detailing all image capture, badge creation, card holder modification, and all photo imaging user functions and responsibilities.
4) Alarm Monitoring Manual - Step-by-step guide and instructions detailing all alarm monitoring system user functions and responsibilities.
5) Technical Maintenance Manual - Shall be a comprehensive and detailed document providing all maintenance action, system testing schedules, troubleshooting flowcharts, functional system layout, and block and schematic diagrams of all system wiring. Technical Maintenance Manual shall also include:
    a. Product Data: Include detailed manufacturer’s product specifications for each component specified. Include data sheets reflecting the model numbers, features, ratings, performance, power requirements, and dimensions.
    b. Shop Drawings: For the Video Security System equipment shall include plans, elevations, sections, details, and attachments to other Work.
    c. Include dimensioned plans and elevation views of components and enclosures. Show access and workspace requirements. Shop drawings shall include mounting details for all racked equipment. Such details shall include all mounting brackets, hardware, and connections to the building.
    d. Wiring Diagrams: Power, signal, and control wiring point-to-point diagrams. Differentiate between manufacturer-installed and field-installed wiring.

    e. Product Certificates: Signed by Manufacturer as Certified for installation of equipment and components certifying that products furnished to The Contractor comply with requirements.
    f. Field Test Reports: Indicate and interpret test results for compliance with performance requirements of installed systems

3.9 System Training

A. Proposal shall include pricing to receive system training on-site by a representative of the SMS manufacturer. Training shall take place before the system is operational as described in the project schedule. A detailed description of the training material shall be included in the submittal package. All training courses shall enable the attendees to be capable of all normal system operations within their respective positions. System Administrators shall receive a course detailing the system functions and operations. Course shall offer configuration training on all aspects of the system including data import-export, reports, card holder management, system workstations, peripherals and field hardware. Photo imaging Users shall receive a course detailing the functions and operations of all aspects of credential production, image capture, card holder record management, reports and Workstation peripherals which are part of the photo imaging process. Alarm Monitoring Users shall receive a course detailing the operation of all aspects of alarm and general overview of field hardware.

B. Training shall be provided for the particular equipment or system as required in each associated specification.

C. A training schedule shall be developed and submitted by the Contractor and approved by the City of Austin at least (30) days prior to the planned training.

D. Provide services of manufacturer's technical representative for <insert hours> hours to instruct City of Austin personnel in operation and maintenance of units.

E. Submit training plans and instructor qualifications in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

3.10 Design and Consulting Services

A. Meetings - Contractor shall meet with City of Austin personnel as required to provide design consulting advice, recommendations and design options for the purpose of developing system requirements and functionality. Contractor may invoice for meeting hours and consulting services per Contract pricing schedule.

B. Coordination - Contractor shall provide project coordination services for the duration of the project. Project coordination shall include producing project schedules, coordinating Contractor personnel, coordinating with other trades as needed, responding to requests for information and clarification, coordinating billing and payment questions and issues, and other services as required to ensure successful execution of the scope of work.

3.11 Installation

A. Comply with NECA 1.

B. Measure indicated mounting heights to bottom of unit for suspended items and to center of unit for wall-mounting items.

C. Headroom Maintenance: If mounting heights or other location criteria are not indicated, arrange and install components and equipment to provide maximum possible headroom consistent with these requirements.

D. Equipment: Install to facilitate service, maintenance, and repair or replacement of components of both electronic safety and security equipment and other nearby installations. Connect in such a way as to facilitate future disconnecting with minimum interference with other items in the vicinity.

E. Right of Way: Give to piping systems installed at a required slope.

F. Equipment location shall be as close as practical to locations shown on the drawings.

G. Inaccessible Equipment:

1. Where the City of Austin determines that the Contractor has installed equipment not conveniently accessible for operation and maintenance, the equipment shall be removed and reinstalled as directed at no additional cost to the City of Austin.

2. "Conveniently accessible" is defined as being capable of being reached without the use of ladders, or without climbing or crawling under or over obstacles such as, but not limited to, motors, pumps, belt guards, transformers, piping, ductwork, conduit and raceways.

3.12 Firestopping

A. Apply firestopping to penetrations of fire-rated floor and wall assemblies for electronic safety and security installations to restore original fire-resistance rating of assembly. Firestopping materials and installation requirements are specified in Division 07 Section 07 84 00 "Firestopping."

3.13 Commissioning

A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up,and Contractor testing required above.

B. Components provided under this section of the specification will be tested as part of a larger system. Refer to section 28 08 00 – COMMISIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for Contractor responsibilities for system commissioning.

3.14 Work Performance

A. Job site safety and worker safety is the responsibility of the contractor.

B. For work on existing stations, arrange, phase and perform work to assure electronic safety and security service for other buildings at all times..

C. New work shall be installed and connected to existing work neatly and carefully. Disturbed or damaged work shall be replaced or repaired to its prior conditions.,

D. Coordinate location of equipment and conduit with other trades to minimize interferences..

3.15 System Programming

A. General Programming Requirements - The Contractor shall be responsible for providing all setup, configuration, and programming to include data entry for the Security Management System (SMS) and subsystems [(e.g., video matrix switch, intercoms, digital video recorders, intrusion devices, including integration of subsystems to the SMS (e.g., camera call up, time synchronization, intercoms)]. System programming for existing or new SMS servers shall not be conducted at the project site.

B. Level of Effort for Programming - The Contractor shall perform and complete system programming (including all data entry) at an offsite location using the Contractor's own copy of the SMS software. The Contractor's copy of the SMS software shall be of the Owners current version. Once system programming has been completed, the Contractor shall deliver the programming data to the City of Austin as electronic medium, utilizing data from the contract documents. The Contractor shall not upload system programming until the City of Austin has provided written approval. The Contractor is responsible for backing up the system prior to uploading new programming data. Additional programming requirements are provided as follows:

    1. Programming for New SMS Server: The Contractor shall provide all other system related programming. The Contractor will be responsible for uploading personnel information (e.g., ID Cards backgrounds, names, access privileges, personnel photos, access schedules, personnel groupings) along with coordinating with City of Austin for device configurations, standards, and groupings. City of Austin willprovide database to support Contractor's data entry tasks. The Contractor shall anticipate a weekly coordination meeting and working with City of Austin to ensure data uploading is performed without incident of loss of function or data loss.

    2. Programming for Existing SMS Servers: The Contractor shall perform all related system programming except for personnel data as noted. The Contractor will not be responsible for uploading personnel information (e.g., ID Cards backgrounds, names, access privileges, access schedules, personnel groupings). The Contractor shall anticipate a weekly coordination meeting and working alongside of City of Austin to ensure data uploading is performed without incident of loss of function or data loss. System programming for SMS servers shall be performed by using the Contractor's own server and software. These servers shall not be connected to existing devices or systems at any time.

C. The Contractor shall identify and request from the City of Austin, any additional data needed to provide a complete and operational system as described in the contract documents.

D. Contractor and City of Austin will coordinate to ensure programming is performed in accordance with City of Austin requirements and programming uploads do not disrupt existing systems functionality. Contractor shall ensure data uploading is performed without incident of loss of function or data loss.

- - - E N D - - -

28 05 13 CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0. City of Austin, Texas

January, 2014

1 PART 1 - GENERAL

1.1 Description

A. This section specifies the finishing, installation, connection, testing and certification the conductors and cables required for a fully functional for electronic safety and security (ESS) system.

1.2 Related Work

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

C. Section 28 05 00 – COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. Requirements for general requirements that are common to more than one section in Division 28.

D. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for personnel safety and to provide a low impedance path for possible ground fault currents.

E. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SECURITY AND SAFETY. Requirements for infrastructure.

F. Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. Requirements for commissioning.

G. Section 31 20 00 - EARTH MOVING. For excavation and backfill for cables that are installed in conduit.

1.3 Definitions

A. BICSI: Building Industry Consulting Service International.

B. EMI: Electromagnetic interference.

C. IDC: Insulation displacement connector.

D. Ladder Cable Tray: A fabricated structure consisting of two longitudinal side rails connected by individual transverse members (rungs).

E. Low Voltage: As defined in NFPA 70 for circuits and equipment operating at less than 50 V or for remote-control and signaling power-limited circuits.

F. Open Cabling: Passing telecommunications cabling through open space (e.g., between the studs of a wall cavity).

G. RCDD: Registered Communications Distribution Designer.

H. Solid-Bottom or Nonventilated Cable Tray: A fabricated structure consisting of integral or separate longitudinal side rails, and a bottom without ventilation openings.

I. Trough or Ventilated Cable Tray: A fabricated structure consisting of integral or separate longitudinal rails and a bottom having openings sufficient for the passage of air and using 75 percent or less of the plan area of the surface to support cables.

J. UTP: Unshielded twisted pair.

1.4 Quality Assurance

A. See section 28 05 00, Paragraph 1.4.

1.5 Submittals

A. In accordance with Section 01 33 23, SHOP DRAWINGS, PRODUCT DATA, AND SAMPLES, furnish the following:

1. Manufacturer's Literature and Data: Showing each cable type and rating.
2. Shop Drawings: Cable tray layout, showing cable tray routes

1.6 Applicable Publications

A. Publications listed below (including amendments, addenda, revisions, supplements and errata) form a part of this specification to the extent referenced. Publications are reference in the text by the basic designation only.

1. American Society of Testing Material (ASTM):

D2301-04 Standard Specification for Vinyl Chloride Plastic Pressure Sensitive Electrical Insulating Tape

2. Federal Specifications (Fed. Spec.):

A-A-59544-08 Cable and Wire, Electrical (Power, Fixed Installation)

3. National Fire Protection Association (NFPA):

70-11	National Electrical Code (NEC)

4. Underwriters Laboratories, Inc. (UL):

44-05	Thermoset-Insulated Wires and Cables
83-08	Thermoplastic-Insulated Wires and Cables
467-07	Electrical Grounding and Bonding Equipment
486A-03	Wire Connectors and Soldering Lugs for Use with Copper Conductors
486C-04	Splicing Wire Connectors
486D-05	Insulated Wire Connector Systems for Underground Use or in Damp or Wet Locations
486E-00	Equipment Wiring Terminals for Use with Aluminum and/or Copper Conductors
493-07	Thermoplastic-Insulated Underground Feeder and Branch Circuit Cable
514B-04	Fittings for Cable and Conduit
1479-03	Fire Tests of Through-Penetration Fire Stops//

1.7 Delivery, Storage and Handling

A. Test cables upon receipt at Project site.

  1. Test each multi-conductor cable for open and short circuits.

1.7 Project Conditions

A. Environmental Limitations: Do not deliver or install UTP, optical fiber, and coaxial cables and connecting materials until wet work in spaces is complete and dry, and temporary HVAC system is operating and maintaining ambient temperature and humidity conditions at occupancy levels during the remainder of the construction period.

2 PART 2 - PRODUCTS

2.1 General

A. Support of Open Cabling:

  1. NRTL labeled for support of [Category 5e] [Category 6] cabling, designed to prevent degradation of cable performance and pinch points that could damage cable.
  2. Support brackets with cable tie slots for fastening cable ties to brackets.
  3. Lacing bars, spools, J-hooks, and D-rings.
  4. Straps and other devices.

2.2 Cable Trays:

A. Cable Tray Materials: Metal, suitable for indoors, and protected against corrosion by [electroplated zinc galvanizing, complying with ASTM B 633, Type 1, not less than 0.000472 inch (0.012 mm) thick] [hot-dip galvanizing, complying with ASTM A 123/A 123M Grade 0.55, not less than 0.002165 inch (0.055 mm) thick].

B. Basket Cable Trays: [6 inches (150 mm) wide and 2 inches (50 mm) deep] <Insert dimensions>. Wire mesh spacing shall not exceed 2 by 4 inches (50 by 100 mm).

C. Trough Cable Trays: [Nominally 6 inches (150 mm)] <Insert dimension> wide.

D. Ladder Cable Trays: [Nominally 18 inches (455 mm)] <Insert dimension> wide, and a rung spacing of [12 inches (305 mm)] <Insert spacing>.

E. Channel Cable Trays: One-piece construction, [nominally 4 inches (100 mm)] <Insert dimension> wide. Slot spacing shall not exceed 4-1/2 inches (115 mm) o.c.

F. Solid-Bottom Cable Trays: One-piece construction, [nominally 12 inches (305 mm)] <Insert dimension> wide. Provide [with] [without] solid covers.

2.3 Conduits and Boxes

A. Comply with requirements in Division 28 Section "Conduits and Backboxes for Electrical Systems."[Flexible metal conduit shall not be used.]

B. Outlet boxes shall be no smaller than 2 inches (50 mm) wide, 3 inches (75 mm) high, and 2-1/2 inches (64 mm) deep.

2.4 Backboards

A. Backboards: Plywood, [fire-retardant treated,] 3/4 by 48 by 96 inches (19 by 1220 by 2440 mm). Comply with requirements for plywood backing panels in Division 06 Section "Rough Carpentry".

2.5 UTP Cable

A. See Division 27

2.6 UTP cable hardware

A. See Division 27

2.7 Optical Fiber Cable

A. See Division 27

2.8 Optical Fiber Cable Hardware

A. See Division 27

2.9 Coaxial Cable

A. General Coaxial Cable Requirements: Broadband type, recommended by cable manufacturer specifically for broadband data transmission applications. Coaxial cable and accessories shall have 75-ohm nominal impedance with a return loss of 20 dB maximum from 7 to 806 MHz.

B. RG-11/U: NFPA 70, Type CATV.

1. No. [14] <Insert size> AWG, solid, copper-covered steel conductor.
2. Gas-injected, foam-PE insulation.
3. Double shielded with 100 percent aluminum polyester tape and 60 percent aluminum braid.
4. Jacketed with sunlight-resistant, black PVC or PE.
5. Suitable for outdoor installations in ambient temperatures ranging from minus 40 to plus 85 deg C.

C. RG59/U: NFPA 70, Type CATVR.

1. No. [20] <Insert size> AWG, solid, silver-plated, copper-covered steel conductor.
2. Gas-injected, foam-PE insulation.
3. Triple shielded with 100 percent aluminum polyester tape and 95 percent aluminum braid; covered by aluminum foil with grounding strip.
4. Color-coded PVC jacket.

D. RG-6/U: NFPA 70, Type CATV or CM.

1. No. [16] <Insert size> AWG, solid, copper-covered steel conductor; gas-injected, foam-PE insulation.
2. Double shielded with 100 percent aluminum-foil shield and 60 percent aluminum braid.
3. Jacketed with black PVC or PE.
4. Suitable for indoor installations.

E. RG59/U: NFPA 70, Type CATV.

1. No. [20] <Insert size> AWG, solid, copper-covered steel conductor; gas-injected, foam-PE insulation.
2. Double shielded with 100 percent aluminum polyester tape and 40 percent aluminum braid.
3. PVC jacket.

F. RG59/U (Plenum Rated): NFPA 70, Type CMP.

  1. No. [20] <Insert size> AWG, solid, copper-covered steel conductor; foam fluorinated ethylene propylene insulation.
  2. Double shielded with 100 percent aluminum-foil shield and 65 percent aluminum braid.
  3. Copolymer jacket.

G. NFPA and UL compliance, listed and labeled by an NRTL acceptable to authorities having jurisdiction as complying with UL 1655, and with NFPA 70 "Radio and Television Equipment" and "Community Antenna Television and Radio Distribution" Articles. Types are as follows:

  1. CATV Cable: Type CATV[, or CATVP or CATVR].
  2. CATV Plenum Rated: Type CATVP, complying with NFPA 262.
  3. CATV Riser Rated: Type CATVR[; or CATVP, CATVR, or CATV], complying with UL 1666.
  4. CATV Limited Rating: Type CATVX.

2.10 Coaxial Cable Hardware

A. Coaxial-Cable Connectors: Type BNC, 75 ohms.

2.11 RS-232 Cable

A. Standard Cable: NFPA 70, Type CM.

  1. Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors.
  2. Polypropylene insulation.
  3. Individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage.
  4. PVC jacket.
  5. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
  6. Flame Resistance: Comply with UL 1581.

B. Plenum-Rated Cable: NFPA 70, Type CMP.

  1. Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors.
  2. Plastic insulation.
  3. Individual aluminum foil-polyester tape shielded pairs with 100 percent shield coverage.
  4. Plastic jacket.
  5. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.
  6. Flame Resistance: Comply with NFPA 262.

2.12 RS-485 CABLE

A. Standard Cable: NFPA 70, Type CM[or CMG].

1. Paired, 2 pairs, twisted, No. 22 AWG, stranded (7x30) tinned copper conductors.
2. PVC insulation.
3. Unshielded.
4. PVC jacket.
5. Flame Resistance: Comply with UL 1581.

B. Plenum-Rated Cable: NFPA 70, Type CMP.

1. Paired, 2 pairs, No. 22 AWG, stranded (7x30) tinned copper conductors.
2. Fluorinated ethylene propylene insulation.
3. Unshielded.
4. Fluorinated ethylene propylene jacket.
5. Flame Resistance: NFPA 262, Flame Test.

2.13 Low Voltage Control Cable

A. Paired Lock Cable: NFPA 70, Type CMG.

1. 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors.
2. PVC insulation.
3. Unshielded.
4. PVC jacket.
5. Flame Resistance: Comply with UL 1581.

B. Plenum-Rated, Paired Lock Cable: NFPA 70, Type CMP.

1. 1 pair, twisted, No. 16 AWG, stranded (19x29) tinned copper conductors.
2. PVC insulation.
3. Unshielded.
4. PVC jacket.
5. Flame Resistance: Comply with NFPA 262.

C. Paired Lock Cable: NFPA 70, Type CMG.

1. 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors.
2. PVC insulation.

    3. Unshielded.
    4. PVC jacket.
    5. Flame Resistance: Comply with UL 1581.
D. Plenum-Rated, Paired Lock Cable: NFPA 70, Type CMP.
    1. 1 pair, twisted, No. 18 AWG, stranded (19x30) tinned copper conductors.
    2. Fluorinated ethylene propylene insulation.
    3. Unshielded.
    4. Plastic jacket.
    5. Flame Resistance: NFPA 262, Flame Test.

2.14 Control Circuit Conductors

A. Class 1 Control Circuits: Stranded copper, Type THHN-THWN, in raceway complying with UL 83.

B. Class 2 Control Circuits: Stranded copper, [Type THHN-THWN, in raceway] [power-limited cable, concealed in building finishes] [power-limited tray cable, in cable tray] complying with UL 83.

C. Class 3 Remote-Control and Signal Circuits: Stranded copper, Type TW or TF, complying with UL 83.

2.15 Identification Products

A. Comply with UL 969 for a system of labeling materials, including label stocks, laminating adhesives, and inks used by label printers.

2.16 Wire Lubricating Compound

A. Suitable for the wire insulation and conduit it is used with, and shall not harden or become adhesive.

B. Shall not be used on wire for isolated type electrical power systems.

2.17 Fireproofing Tape

A. The tape shall consist of a flexible, conformable fabric of organic composition coated one side with flame-retardant elastomer.

B. The tape shall be self-extinguishing and shall not support combustion. It shall be arc-proof and fireproof.

C. The tape shall not deteriorate when subjected to water, gases, salt water, sewage, or fungus and be resistant to sunlight and ultraviolet light.

D. The finished application shall withstand a 200-ampere arc for not less than 30 seconds.

E. Securing tape: Glass cloth electrical tape not less than 0.18 mm (7 mils) thick, and 19 mm (3/4 inch) wide.

3 PART 3 - EXECUTION

3.1 INSTALLATION of conductors and cables

A. Comply with NECA 1.

B. General Requirements for Cabling:

C. Comply with TIA/EIA-568-B.1.

D. Comply with BICSI ITSIM, Ch. 6, "Cable Termination Practices."

E. Install 110-style IDC termination hardware unless otherwise indicated.

F. Terminate all conductors; no cable shall contain un-terminated elements. Make terminations only at indicated outlets, terminals, and cross-connect and patch panels.

G. Cables may not be spliced. Secure and support cables at intervals not exceeding 30 inches (760 mm) and not more than 6 inches (150 mm) from cabinets, boxes, fittings, outlets, racks, frames, and terminals.

H. Bundle, lace, and train conductors to terminal points without exceeding manufacturer's limitations on bending radii, but not less than radii specified in BICSI ITSIM, "Cabling Termination Practices" Chapter. Install lacing bars and distribution spools.

I. Do not install bruised, kinked, scored, deformed, or abraded cable. Do not splice cable between termination, tap, or junction points. Remove and discard cable if damaged during installation and replace it with new cable.

J. Cold-Weather Installation: Bring cable to room temperature before dereeling. Heat lamps shall not be used for heating.

K. Pulling Cable:

  1. Comply with BICSI ITSIM, Ch. 4, "Pulling Cable." Monitor cable pull tensions.

  2. Provide installation equipment that will prevent the cutting or abrasion of insulation during pulling of cables.

  3. Use ropes made of nonmetallic material for pulling feeders.

  4. Attach pulling lines for feeders by means of either woven basket grips or pulling eyes attached directly to the conductors, as approved by the Resident Engineer/COTR.

  5. Pull in multiple cables together in a single conduit.

L. Splice cables and wires where necessary only in outlet boxes, junction boxes, or pull boxes.

   1. Splices and terminations shall be mechanically and electrically secure.
   2. Where the City of Austin City of Austin determines that unsatisfactory splices or terminations have been installed, remove the devices and install approved devices at no additional cost to the City of Austin .

M. Seal cable and wire entering a building from underground, between the wire and conduit where the cable exits the conduit, with a non-hardening approved compound.

N. Unless otherwise specified in other sections install wiring and connect to equipment/devices to perform the required functions as shown and specified.

O. System voltages shall be 120 volts or lower where shown on the drawings or as required by the NEC.

P. Open-Cable Installation:

   1. Install cabling with horizontal and vertical cable guides in telecommunications spaces with terminating hardware and interconnection equipment.
   2. Suspend copper cable not in a wireway or pathway a minimum of 8 inches (200 mm) above ceilings by cable supports not more than [60 inches (1525 mm)] <Insert dimension> apart.
   3. Cable shall not be run through structural members or in contact with pipes, ducts, or other potentially damaging items.

Q. Installation of Cable Routed Exposed under Raised Floors:

   1. Install plenum-rated cable only.
   2. Install cabling after the flooring system has been installed in raised floor areas.
   3. Coil cable [72 inches (1830 mm)] <Insert size> long shall be neatly coiled not less than [12 inches (300 mm)] <Insert size> in diameter below each feed point.

R. Outdoor Coaxial Cable Installation:

   1. Install outdoor connections in enclosures complying with NEMA 250, Type 4X. Install corrosion-resistant connectors with properly designed O-rings to keep out moisture.
   2. Attach antenna lead-in cable to support structure at intervals not exceeding 36 inches (915 mm).

S. Separation from EMI Sources:

   1. Comply with BICSI TDMM and TIA/EIA-569-A recommendations for separating unshielded copper voice and data communication cable from potential EMI sources, including electrical power lines and equipment.

2. Separation between open communications cables or cables in nonmetallic raceways and unshielded power conductors and electrical equipment shall be as follows:
    a. Electrical Equipment Rating Less Than 2 kVA: A minimum of 5 inches (127 mm).
    b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 12 inches (300 mm).
    c. Electrical Equipment Rating More Than 5 kVA: A minimum of 24 inches (600 mm).
3. Separation between communications cables in grounded metallic raceways and unshielded power lines or electrical equipment shall be as follows:
    a. Electrical Equipment Rating Less Than 2 kVA: A minimum of 2-1/2 inches (64 mm).
    b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 6 inches (150 mm).
    c. Electrical Equipment Rating More Than 5 kVA: A minimum of 12 inches (300 mm).
4. Separation between communications cables in grounded metallic raceways and power lines and electrical equipment located in grounded metallic conduits or enclosures shall be as follows:
    a. Electrical Equipment Rating Less Than 2 kVA: No requirement.
    b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 3 inches (75 mm).
    c. Electrical Equipment Rating More Than 5 kVA: A minimum of 6 inches (150 mm).
5. Separation between Cables and Electrical Motors and Transformers, 5 k or HP and Larger: A minimum of 48 inches (1200 mm).
6. Separation between Cables and Fluorescent Fixtures: A minimum of 5 inches (127 mm).

3.2 Control Circuit Conductors

A. Minimum Conductor Sizes:
    1. Class 1 remote-control and signal circuits, No. 14 AWG.
    2. Class 2 low-energy, remote-control and signal circuits, No. 16 AWG.
    3. Class 3 low-energy, remote-control, alarm and signal circuits, No. 12 AWG.

3.3 Connections

A. Comply with requirements in Division 28 Section, PHYSICAL ACCESS CONTROL for connecting, terminating, and identifying wires and cables.

B. Comply with requirements in Division 28 Section "INTRUSION DETECTION" for connecting, terminating, and identifying wires and cables.

C. Comply with requirements in Division 28 Section "VIDEO SURVEILLANCE" for connecting, terminating, and identifying wires and cables.

D. Comply with requirements in Division 28 Section "ELECTRONIC PERSONAL PROTECTION SYSTEMS" for connecting, terminating, and identifying wires and cables.

3.4 Firestopping

A. Comply with requirements in Division 07 Section "PENETRATION FIRESTOPPING."

B. Comply with TIA/EIA-569-A, "Firestopping" Annex A.

C. Comply with BICSI TDMM, "Firestopping Systems" Article.

3.5 Grounding and Bonding

A. For communications wiring, comply with ANSI-J-STD-607-A and with BICSI TDMM, "Grounding, Bonding, and Electrical Protection" Chapter.

B. For low-voltage wiring and cabling, comply with requirements in Division 28 Section "GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY."

3.6 Identification

A. Identify system components, wiring, and cabling complying with TIA/EIA-606-A.

B. Install a permanent wire marker on each wire at each termination.

C. Identifying numbers and letters on the wire markers shall correspond to those on the wiring diagrams used for installing the systems.

D. Wire markers shall retain their markings after cleaning.

E. In each handhole, install embossed brass tags to identify the system served and function.

3.7 Field Quality Control

A. Testing Agency: Engage a qualified testing agency to perform tests and inspections.

B. Perform tests and inspections.

C. Tests and Inspections:

  1. Visually inspect UTP and optical fiber cable jacket materials for UL or third-party certification markings. Inspect cabling terminations to confirm color-coding for pin assignments, and inspect cabling connections to confirm compliance with TIA/EIA-568-B.1.
  2. Visually inspect cable placement, cable termination, grounding and bonding, equipment and patch cords, and labeling of all components.

3. Coaxial Cable Tests: Comply with requirements in Division 27 Section "Master Antenna Television System."

D. Document data for each measurement. Print data for submittals in a summary report that is formatted using Table 10.1 in BICSI TDMM as a guide, or transfer the data from the instrument to the computer, save as text files, print, and submit.

E. End-to-end cabling will be considered defective if it does not pass tests and inspections.

F. Prepare test and inspection reports.

3.8 Existing Wiring

A. Unless specifically indicated on the plans, existing wiring shall not be reused for the new installation. Only wiring that conforms to the specifications and applicable codes may be reused. If existing wiring does not meet these requirements, existing wiring may not be reused and new wires shall be installed.

- - - E N D - - -

28 05 26 GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0. City of Austin, Texas

January, 2014

1 PART 1 - GENERAL

1.1 Description

A. This section specifies the finishing, installation, connection, testing and certification of the grounding and bonding required for a fully functional Electronic Safety and Security (ESS) system. All requirements herein are to be fulfilled by the Contractor providing the Grounding Electrode System and Lightning Protection System for the facility.

B. “Grounding electrode system” refers to all electrodes required by NEC, as well as including made, supplementary, grounding electrodes.

C. The terms “connect” and “bond” are used interchangeably in this specification and have the same meaning.

1.2 Related Work

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 26 41 00 - FACILITY LIGHTNING PROTECTION. Requirements for a lightning protection system.

C. Section 28 05 00 - REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY INSTALLATIONS. For general electrical requirements, quality assurance, coordination, and project conditions that are common to more than one section in Division 28.

D. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for low voltage power and lighting wiring.

E. Section 28 08 00 - COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. Requirements for commissioning..

1.3 Quality Assurance

A. See section 28 05 00, Paragraph 1.4.

1.4 Submittals

A. Submit in accordance with Section 28 05 00, COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. Submittals are the responsibility of the Contractor providing the Grounding Electrode System and Lightning Protection System for the facility.

B. Shop Drawings:

   1. Clearly present enough information to determine compliance with drawings and specifications.

   2. Include the location of system grounding electrode connections and the routing of aboveground and underground grounding electrode conductors.

C. Test Reports: Provide certified test reports of ground resistance.

D. Certifications: Two weeks prior to final inspection, submit four copies of the following to the City of Austin:

   1. Certification that the materials and installation are in accordance with the drawings and specifications.

   2. Certification by the contractor that the complete installation has been properly installed and tested.

1.5 Applicable Publications

A. Publications listed below (including amendments, addenda, revisions, supplements, and errata) form a part of this specification to the extent referenced. Publications are referenced in the text by designation only.

B. American Society for Testing and Materials (ASTM):

   1. B1-07 Standard Specification for Hard-Drawn Copper Wire

   2. B3-07 Standard Specification for Soft or Annealed Copper Wire

   3. B8-04 Standard Specification for Concentric-Lay-Stranded Copper Conductors, Hard, Medium-Hard, or Soft

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

   1. 81-1983 IEEE Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System

   2. C2-07 National Electrical Safety Code

D. National Fire Protection Association (NFPA):

   1. 70-11 National Electrical Code (NEC)

   2. 99-2005 Health Care Facilities

E. Underwriters Laboratories, Inc. (UL):

  1. 44-05 Thermoset-Insulated Wires and Cables
  2. 83-08 Thermoplastic-Insulated Wires and Cables
  3. 467-07 Grounding and Bonding Equipment
  4. 486A-486B-03 Wire Connectors

2 PART 2 - PRODUCTS

2.1 GROUNDING AND BONDING CONDUCTORS

A. Equipment grounding conductors shall be UL 83 insulated stranded copper, except that sizes 6 mm² (10 AWG) and smaller shall be solid copper. Insulation color shall be continuous green for all equipment grounding conductors, except that wire sizes 25 mm² (4 AWG) and larger shall be permitted to be identified per NEC.

B. Bonding conductors shall be ASTM B8 bare stranded copper, except that sizes 6 mm² (10 AWG) and smaller shall be ASTM B1 solid bare copper wire.

2.2 GROUND RODS

A. Copper clad steel, 19 mm (3/4-inch) diameter by 3000 mm (10 feet) long, conforming to UL 467.

B. Quantity of rods shall be as required to obtain the specified ground resistance.

2.3 SPLICES AND TERMINATION COMPONENTS

A. Components shall meet or exceed UL 467 and be clearly marked with the manufacturer, catalog number, and permitted conductor size(s).2.4 ground connections

B. Listed and labeled by an NRTL acceptable to authorities having jurisdiction for applications in which used and for specific types, sizes, and combinations of conductors and other items connected.

C. Below Grade: Exothermic-welded type connectors.

D. Above Grade:

  1. Bonding Jumpers: Compression-type connectors, using zinc-plated fasteners and external tooth lockwashers.
  2. Connection to Building Steel: Exothermic-welded type connectors.
  3. Ground Busbars: Two-hole compression type lugs, using tin-plated copper or copper alloy bolts and nuts.

4. Rack and Cabinet Ground Bars: One-hole compression-type lugs, using zinc-plated or copper alloy fasteners.
5. Bolted Connectors for Conductors and Pipes: Copper or copper alloy, pressure type with at least two bolts.
    a. Pipe Connectors: Clamp type, sized for pipe.
6. Welded Connectors: Exothermic-welding kits of types recommended by kit manufacturer for materials being joined and installation conditions.

2.4 EQUIPMENT RACK AND CABINET GROUND BARS

A. Provide solid copper ground bars designed for mounting on the framework of open or cabinet-enclosed equipment racks with minimum dimensions of 4 mm thick by 19 mm wide (3/8 inch x ¾ inch).

2.5 GROUND TERMINAL BLOCKS

A. At any equipment mounting location (e.g., backboards and hinged cover enclosures) where rack-type ground bars cannot be mounted, provide screw lug-type terminal blocks.

SPEC WRITER NOTE: Include Standard Detail on drawings. Edit detail to suit project requirements.

2.6 SPLICE CASE GROUND ACCESSORIES

A. Splice case grounding and bonding accessories shall be supplied by the splice case manufacturer when available. Otherwise, use 16 mm² (6 AWG) insulated ground wire with shield bonding connectors.

2.7 COMPUTER ROOM GROUND

A. Provide 50mm2 (1/0 AWG) bare copper grounding conductors bolted at mesh intersections to form an equipotential grounding grid. The equipotential grounding grid shall form a 600mm (24 inch) mesh pattern. The grid shall be bonded to each of the access floor pedestals.

2.8 SECURITY CONTROL ROOM GROUND

A. Provide 50mm2 (1/0 AWG) stranded copper grounding conductor(s) color coded with a green jacket, bolted at the Control Room’s Communications System Grounding Electrode Cooper Plate and circulate to each equipment rack ground bus bar through the wire management system. Connect each equipment rack, wire management system’s cable tray, ladder, etc. to the circulating ground wire with a minimum 25mm2 (4AWG) stranded Cooper Wire, color coded with a green jacket.
    1. Connect each equipment rack ground buss bar to the circulating ground wire a indicated in 2.9.A, and

2. Connect each additional room item to the circulating ground wire as indicated in 2.9.A.

3 PART 3 - EXECUTION

3.1 GENERAL

A. Ground in accordance with the NEC, as shown on drawings, and as specified herein.

B. System Grounding:

1. Secondary service neutrals: Ground at the supply side of the secondary disconnecting means and at the related transformers.
2. Separately derived systems (transformers downstream from the service entrance):

C. Equipment Grounding: Metallic structures, including ductwork and building steel, enclosures, raceways, junction boxes, outlet boxes, cabinets, machine frames, and other conductive items in close proximity with electrical circuits, shall be bonded and grounded, unless otherwise specified in construction drawings or specifications.

3.2 INACCESSIBLE GROUNDING CONNECTIONS

A. Make grounding connections, which are buried or otherwise normally inaccessible (except connections for which periodic testing access is required) by exothermic weld.

3.3 CORROSION INHIBITORS

A. When making ground and ground bonding connections, apply a corrosion inhibitor to all contact surfaces. Use corrosion inhibitor appropriate for protecting a connection between the metals used.

3.4 CONDUCTIVE PIPING

A. Bond all conductive piping systems, interior and exterior, to the building grounding electrode system. Bonding connections shall be made as close as practical to the equipment ground bus.

3.5 COMPUTER ROOM/SECURITY EQUIPMENT ROOM GROUNDING

A. Conduit: Ground and bond metallic conduit systems as follows:

1. Ground metallic service conduit and any pipes entering or being routed within the computer room at each end using 16 mm² (6AWG) bonding jumpers.
2. Bond at all intermediate metallic enclosures and across all joints using 16 mm² (6 AWG) bonding jumpers.

3.6 WIREWAY GROUNDING

A. Ground and Bond Metallic Wireway Systems as follows:

   1. Bond the metallic structures of wireway to provide 100 percent electrical continuity throughout the wireway system by connecting a 16 mm² (6 AWG) bonding jumper at all intermediate metallic enclosures and across all section junctions.
   2. Install insulated 16 mm² (6 AWG) bonding jumpers between the wireway system bonded as required in paragraph 1 above, and the closest building ground at each end and approximately every 16 meters (50 feet).
   3. Use insulated 16 mm² (6 AWG) bonding jumpers to ground or bond metallic wireway at each end at all intermediate metallic enclosures and cross all section junctions.
   4. Use insulated 16 mm² (6 AWG) bonding jumpers to ground cable tray to column-mounted building ground plates (pads) at each end and approximately every 15 meters.

3.7 LIGHTNING PROTECTION SYSTEM

A. Bond the lightning protection system to earth ground externally to the building. Under no condition shall the electrical system's third of fourth ground electrode system, or the telecommunications system circulating ground system be connected to the lightning protection system. The Facility's structural steel may be used to connect the lightning protection system at the direction of a Resident Engineer certified by an independent certified grounding contractor.

3.8 EXTERIOR LIGHT/CAMERA POLES

A. Provide 20 ft [6.1 M] of No. 4 bare copper coiled at bottom of pole base excavation prior to pour, plus additional unspliced length in and above foundation as required to reach pole ground stud.

3.9 GROUND RESISTANCE

A. Grounding system resistance to ground shall not exceed 5 ohms. Make any modifications or additions to the grounding electrode system necessary for compliance without additional cost to the Government. Final tests shall ensure that this requirement is met.

B. Resistance of the grounding electrode system shall be measured using a four-terminal fall-of-potential method as defined in IEEE 81. Ground resistance measurements shall be made before the electrical distribution system is energized and shall be made in normally dry conditions not fewer than 48 hours after the last rainfall. Resistance measurements of separate grounding electrode systems shall be made before the systems are bonded together below grade. The combined resistance of separate systems may be used to meet the required resistance, but the specified number of electrodes must still be provided.

C. Services at power company interface points shall comply with the power company ground resistance requirements.

D. Below-grade connections shall be visually inspected by the City of Austin prior to backfilling. The contractor shall notify the City of Austin 24 hours before the connections are ready for inspection.

3.10 GROUND ROD INSTALLATION

A. Drive each rod vertically in the earth, not less than 3000 mm (10 feet) in depth.

B. Where permanently concealed ground connections are required, make the connections by the exothermic process to form solid metal joints. Make accessible ground connections with mechanical pressure type ground connectors.

C. Where rock prevents the driving of vertical ground rods, install angled ground rods or grounding electrodes in horizontal trenches to achieve the specified resistance.

3.11 GROUNDING FOR RF/EMI CONTROL

A. Install bonding jumpers to bond all conduit, cable trays, sleeves and equipment for low voltage signaling and data communications circuits. Bonding jumpers shall consist of 100 mm (4 inches) wide copper strip or two 6 mm^2 (10 AWG) copper conductors spaced minimum 100 mm (4 inches) apart. Use 16 mm^2 (6 AWG) copper where exposed and subject to damage.

B. Comply with the following when shielded cable is used for data circuits.

1. Shields shall be continuous throughout each circuit.
2. Connect shield drain wires together at each circuit connection point and insulate from ground. Do not ground the shield.
3. Do not connect shields from different circuits together.
4. Shield shall be connected at one end only. Connect shield to signal reference at the origin of the circuit. Consult with equipment manufacturer to determine signal reference.

3.12 LABELING

A. Comply with requirements in Division 26 Section "ELECTRICAL IDENTIFICATION" Article for instruction signs. The label or its text shall be green.

B. Install labels at the telecommunications bonding conductor and grounding equalizer.

1. Label Text: "If this connector or cable is loose or if it must be removed for any reason, notify the facility manager."

3.13 FIELD QUALITY CONTROL

A. Perform tests and inspections.

B. Tests and Inspections:

   1. After installing grounding system but before permanent electrical circuits have been energized, test for compliance with requirements.

   2. Inspect physical and mechanical condition. Verify tightness of accessible, bolted, electrical connections with a calibrated torque wrench according to manufacturer's written instructions.

   3. Test completed grounding system at each location where a maximum ground-resistance level is specified, at service disconnect enclosure grounding terminal at individual ground rods. Make tests at ground rods before any conductors are connected.

      a. Measure ground resistance no fewer than two full days after last trace of precipitation and without soil being moistened by any means other than natural drainage or seepage and without chemical treatment or other artificial means of reducing natural ground resistance.

      b. Perform tests by fall-of-potential method according to IEEE 81.

C. Grounding system will be considered defective if it does not pass tests and inspections.

D. Prepare test and inspection reports.

E. Excessive Ground Resistance: If resistance to ground exceeds specified values, notify Architect promptly and include recommendations to reduce ground resistance.

F. Report measured ground resistances that exceed the following values:

1. Power Distribution Units or Panel boards Serving Electronic Equipment: 3 ohm(s).

2. Manhole Grounds: 10 ohms.

- - - E N D - - -

28 08 00 COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0. City of Austin, Texas

January, 2014

1 PART 1 - GENERAL

1.1 DESCRIPTION

A. The requirements of this Section apply to all sections of Division 28.

B. This project will have selected building systems commissioned. The City of Austin and the Contractor will negotiate the need for commissioning at the outset of selected new scopes of work.

1.2 SUMMARY

A. This Section includes requirements for commissioning the Facility electronic safety and security systems, related subsystems and related equipment.

1.3 COMMISSIONED SYSTEMS

A. Commissioning of a system or systems specified in Division 28 is part of the construction process. Documentation and testing of these systems, as well as training of the CITY OF AUSTIN's Operation and Maintenance personnel, is required in cooperation with the CITY OF AUSTIN.

1.4 SUBMITTALS

A. The commissioning process requires review of selected Submittals that pertain to the systems to be commissioned. The Commissioning Agent will provide a list of submittals that will be reviewed by the City. This list will be reviewed and approved by the CITY OF AUSTIN prior to forwarding to the Contractor.

2 PART 2 - PRODUCTS (NOT USED)

3 PART 3 - EXECUTION

3.1 CONSTRUCTION INSPECTIONS

A. Commissioning of Electronic Safety and Security systems will require inspection of individual elements of the electronic safety and security systems throughout the construction period. The Contractor shall coordinate with the City of Austin in accordance with the Commissioning plan to schedule electronic safety and security systems inspections as required to support the Commissioning Process.

3.2 PRE-FUNCTIONAL CHECKLISTS

A. The Contractor shall complete Pre-Functional Checklists to verify systems, subsystems, and equipment installation is complete and systems are ready for Systems Functional Performance Testing. The ontractor will provide copies of the Pre-Functional Checklists to the City to be used to document equipment installation. The Contractor shall complete the checklists. Completed checklists shall be submitted to the CITY OF AUSTIN for review. The City of Austin may spot check a sample of completed checklists. If the ity determines that the information provided on the checklist is not accurate, the City will return the marked-up checklist to the Contractor for correction and resubmission. If the City determines that a significant number of completed checklists for similar equipment are not accurate, the City will select a broader sample of checklists for review. If the City determines that a significant number of the broader sample of checklists is also inaccurate, all the checklists for the type of equipment will be returned to the Contractor for correction and resubmission.

3.3 CONTRACTOR’S TESTS

A. Contractor tests as required by other sections of Division 28 shall be scheduled and documented. All testing shall be incorporated into the project schedule. Contractor shall provide no less than (7) calendar days’ notice of testing. The City of Austin will witness selected Contractor tests at the sole discretion of the City. Contractor tests shall be completed prior to scheduling Systems Functional Performance Testing.

3.4 SYSTEMS FUNCTIONAL PERFORMANCE TESTING

A. The Commissioning Process includes Systems Functional Performance Testing that is intended to test systems functional performance under steady state conditions, to test system reaction to changes in operating conditions, and system performance under emergency conditions. The City will prepare detailed Systems Functional Performance Test procedures for review and comment by the Contractor. The Contractor shall provide the required labor, materials, and test equipment identified in the test procedure to perform the tests. The City will witness and document the testing. The Contractor and the City shall sign the test reports to verify tests were performed.

3.5 TRAINING OF CITY OF AUSTIN PERSONNEL

A. Training of the CITY OF AUSTIN operation and maintenance personnel is required prior to Acceptance of installed systems. The Contractor shall provide competent, factory-authorized personnel to provide instruction to operation and maintenance personnel concerning the location, operation, and troubleshooting of the installed systems. The instruction shall be scheduled in coordination with the CITY OF AUSTIN after submission and approval of formal training plans.

----- END -----

28 13 00 PHYSICAL ACCESS CONTROL FOR ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0. City of Austin, Texas

January, 2014

1 PART 1 – GENERAL

1.1 DESCRIPTION

A. This section specifies the finishing, installation, connection, testing and certification of a complete and fully operating Physical Access Control System, hereinafter referred to as the PACS.

B. This Section includes a PACS consisting of one or more system server (s), one or more networked workstation computers, operating system and ESS application software, and field-installed Controllers connected by a high-speed electronic data transmission network. The PACS shall have the following:

1. PhysicalAccess Control - Regulating access through doors, gates , traffic-control bollards, turnstiles, roof hatches, traffic gates, and other pass-through barriers. The PACS functions may consist of one or more of the following:
    a. Anti-passback
    b. Visitor assignment
    c. Surge protection
    d. Secondary alarm annunciator
    e. Credential cards and readers
    f. Push-button switches
    g. Credential creation and credential holder database and management
    h. Monitoring of field-installed devices
    i. Interface with elevator control, burglar alarm systems, and/or video cameras
    j. Reporting
    k. Tamper protection

        l. Sensors
        m. Power supplies
        n. Electric door strikes/mortises
        o. Intelligent controller (s)
    2. Security:
        a. Real-time guard tour.
        b. Time and attendance.
        c. Key tracking.
        d. Video and camera control.
        e. Time and attendance
        f. Software-enabled door/gate controls

C. System Architecture

    1. Criticality, operational requirements, and/or limiting points of failure may dictate the development of an enterprise and regional server architecture as opposed to system capacity. Provide server and workstation configurations with all necessary connectors, interfaces and accessories as shown.

D. PACS shall provide secure and reliable identification of City of Austin employees, authorized visitors, temporary employees, and contractors by utilizing credential authentication.

E. Physical Access Control System (PACS) components may include:

    1. Head-End (enterprise) equipment server (s)/workstation (s),
    2. One or more networked PC-based workstations,
    3. Physical Access Control System and Database Management Software,
    4. Credential validation software/hardware,
    5. Field installed controllers,
    6. Card readers,
    7. HID iClass Corporate 1000-registered identification badges, cards, fobs.
    8. Supportive information system,
    9. Door locks and sensors,
    10. Power supplies,
    11. PACS system may interface with:
        a. Video Surveillance and Assessment System (VSAS),

    b. Gate, turnstile, and traffic arm controls,
    c. Automatic door operators,
    d. Intrusion Detection System (IDS),
    e. Intercommunication System (Intercom),
    f. Elevator Controls,
    g. Other sub-systems as required

F. Head-End equipment server, workstations and controllers shall be connected by a high-speed electronic data transmission network provided by the City of Austin.

G. Information system supporting PACS , Head-End equipment server (s), workstations, network switches, routers and controllers will be provided by the City of Austin. Contractor shall coordinate with the City to ensure that network devices, server (s) and workstation (s) are compliant with manufacturers' recommended specifications.

H. PACS system shall support:

1. Multiple credential authentication modes;
2. Bidirectional communication with the reader;
3. Incident response policy implementation capability; system shall have capability to automatically change access privileges for certain user groups to high security areas in case of incident/emergency;
4. Visitor management;
5. ESS software license tracking and management;
6. Real-time on-screen display of access control device statuses via icons or indicators overlayed on on-screen images (floor plans);
7. On-screen icons or indicators shall be user interactive, allowing users to control the devices via mouse clicks and/or keyboard commands;
8. User-configurable schedules for access control devices (locks and actuators), including the ability to configure holidays;
9. Provide multiple levels of system security permissions that are user-configurable depending system user roles and responsibilities;
10. Integration to video recording system to trigger video recording capabilities based on events or alarms; this capability shall be user-configurable;
11. Free-text entry fields within the user software for annotating events, entering narratives, or entering comments;
12. User software shall display a credential-holder's photograph based on user-defined access control events;

13. User creating of system user groups based defined system user roles;
14. Allow simultaneous viewing of the same system data by multiple users without compromising system performance or data integrity;
15. Allow system operators to perform multiple tasks such as badge creation, facility monitoring, manual control of devices) under a single login session;
16. Configurable guard tours (making rounds, check-ins, return to post);
17. Indicate failed or inoperative components attached to the system;
18. Ability to use Dept. of Homeland Security threat levels to automatically change configurations and profiles;
19. Capability to record swquential, repeated credential presentations (card swipes);
20. Visitor management capability;
21. Provide support for two-person entry control;
22. Notifications to system administrators when software or hardware components become non-functional;

I. All security-relevant decisions shall be made on “secure side of the door”. Secure-side processing shall include;

1. Challenge/response management,
2. PKI path discovery and validation,
3. Credential identifier processing,
4. Authorization decisions.

J. System Software Operating Systems: Schneider Electric Continuum application software, and Microsoft Windows Server OS for servers and head-end workstations, .

K. Software shall have the following capabilities:

1. Multiuser and multitasking to allow for independent activities and monitoring to occur simultaneously at different workstations.
2. Support authentication and enrollment, including;
    a. Expiration date check,
    b. Digital photo display/check,
    c. Card scanner capability
3. Automatically deny access to any revoked credential in the system.
4. Graphical user interface

    5. System license (s) shall be for the entire system provided under this scope of work, and shall include capability for future additions that are within the indicated system size limits specified in this Section.
    6. System shall have open architecture that allows importing and exporting of data and interfacing with other systems that are compatible with Schneider Electric Continuum software.
    7. Operator login and access shall be effected via integration with the City's Microsoft Active Directory and password protection.

L. Systems Networks:
  1. A STANDALONE ESS installation shall interconnect all components of the system on a single data network. This network shall include communications between a central station and any peer or subordinate workstations, enrollment stations, local annunciation stations, portal control stations or redundant central stations.
  2. An ENTERPRISE ESS installation shall interconnect all components of the building or campus ESS on one or more local area networks that are, in turn, connected to the City's ESS network. Communications between site workstations, enrollment stations, local annunciation station, portal control stations and other components shall be on the local area network. Communications from the building or campus central station, and intelligent controllers to the enterprise SMS Server (s) shall be over the wide area ESS network.

  M. Security Management System Server Redundancy:
    1. The SMS shall support multiple levels of fault tolerance and SMS redundancy listed and described below:
      a. Hot Standby Servers
      b. Clustering
      c. Disk Mirroring
      d. RAID Level 10
      e. Distributed Intelligence
      f. Distributed load

  N. Number of points:
    1. PACS shall support multiple autonomous regional servers that can connect to a master command and controller server and a master database server.
    2. Unlimited number of access control readers, unlimited number of inputs or outputs, unlimited number of client workstations, unlimited number of cardholders.

3. Total system solution to enable enterprise-wide, networked, multi-user access to all system resources via a wide range of options for connectivity with the customer’s existing LAN and WAN.

O. Network(s) connecting PCs and Controllers shall consist of one or more of the following:

1. Local area, IEEE 802.3 Fast Ethernet [10 BASE-T] [100 BASE-TX], star topology network based on TCP/IP.

1.2 RELATED WORK

A. SPEC WRITER NOTE: Delete any item or paragraph not applicable in the section and renumber the paragraphs.

B. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

C. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

D. Section 08 11 73 - SLIDING METAL FIRE DOORS. Requirements for door installation.

E. Section 08 34 59 - VAULT DOORS AND DAY GATES. Requirements for door and gate installation.

F. Section 08 35 13.13 - ACCORDIAN FOLDING DOORS. Requirements for door installation.

G. Section 08 71 00 - DOOR HARDWARE. Requirements for door installation.

H. Section 10 14 00 - SIGNAGE. Requirements for labeling and signs.

I. Section 14 21 00 ELECTRIC TRACTION ELEVATORS. Requirements for elevators.

J. Section 14 24 00 - HYDRAULIC ELEVATORS. Requirements for elevators.

K. Section 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.

L. Section 26 05 21 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW). Requirements for power cables.

M. Section 26 05 33 – RACEWAYS AND BOXES FOR ELECTRICAL SYSTEMS. Requirements for infrastructure.

N. Section 26 05 41 - UNDERGROUND ELECTRICAL CONSTRUCTION. Requirements for underground installation of wiring.

O. Section 26 56 00 - EXTERIOR LIGHTING. Requirements for perimeter lighting.

P. Section 28 05 00 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. For general requirements that are common to more than one section in Division 28.

Q. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

R. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

S. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.

T. Section 28 08 00 - COMMISIONING OF ELECTRONIC SAFETY AND SECURITY. For requirements for commissioning, systems readiness checklists, and training.

U. Section 28 13 16 - ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT. Requirements for control and operation of all security systems.

V. Section 28 13 53 - SECURITY ACCESS DETECTION. Requirements for screening of personnel and shipments.

W. Section 28 16 00 - INTRUSION DETECTION SYSTEM (IDS). Requirements for alarm systems.

X. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

Y. Section 28 26 00 - ELECTRONIC PERSONAL PROTECTION SYSTEM (EPPS). Requirements for emergency and interior communications.

Z. Section 28 31 00 - FIRE DETECTION AND ALARM. Requirements for integration with fire detection and alarm system.

1.3 QUALITY ASSURANCE

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1

1.4 SUBMITTALS

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, PART 1

1.5 APPLICABLE PUBLICATIONS

A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1

1.6 DEFINITIONS

A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1

1.7 COORDINATION

A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1

1.8 MAINTENANCE AND SERVICE

A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1

1.9 PERFORMANCE REQUIREMENTS

A. PACS shall provide support for multiple authentication modes and bidirectional communication with the reader. PACS shall provide implementation capability for enterprise security policy and incident response.

B. All processing of authentication information must occur on the “safe side” of a door

C. Physical Access Control System shall provide access to following Security Areas:

  1. Controlled Areas
  2. Limited Areas
  3. Exclusion Areas

D. PACS shall provide:

  1. Single-factor authentication for access to Controlled security areas
  2. Two-factor authentication for access to Limited security areas
  3. Three-factor authentication for access to Exclusion security areas

E. Distributed Processing: System shall be a fully distributed processing system so that information, including time, date, valid codes, access levels, and similar data, is downloaded to Controllers so that each Controller makes access-control decisions for that Location. Do not use intermediate Controllers for physical access control. If communications to Central Station are lost, all Controllers shall automatically buffer event transactions and access-related data until communications are restored, at which time buffered events shall be uploaded to the Central Station, and data will be refreshed from the Central Station to the Controllers.

F. Number of Locations: Support unlimited number of separate Locations using a single PC with combinations of direct-connect, dial-up, or TCP/IP LAN connections to each Location.

  1. Each Location shall have its own database and history in the Central Station. Locations may be combined to share a common database.

G. System Network Requirements:

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

H. Central Station shall provide operator interface, interaction, display, control, and dynamic and real-time monitoring. Central Station shall control system networks to interconnect all system components, including workstations and field-installed Controllers.

I. Field equipment shall include Controllers, sensors, and controls. Controllers shall serve as an interface between the Central Station and sensors and controls. Data exchange between the Central Station and the Controllers shall include down-line transmission of commands, software, and databases to Controllers. The up-line data exchange from the Controller to the Central Station shall include status data such as intrusion alarms, status reports, and entry-control records. Controllers are classified as alarm-annunciation or entry-control type.

J. False Alarm Reduction: The design of Central Station and Controllers shall contain features to reduce false alarms. P. Error Detection: A cyclic code error detection method shall be used between Controllers and the Central Station, which shall detect single- and double-bit errors, burst errors of eight bits or less, and at least 99 percent of all other multibit and burst error conditions. Interactive or product error detection codes alone will not be acceptable. A message shall be in error if one bit is received incorrectly. System shall retransmit messages with detected errors. A two-digit decimal number shall be operator assignable to each communication link representing the number of retransmission attempts. When the number of consecutive retransmission attempts equals the assigned quantity, the Central Station shall print a communication failure alarm message. System shall monitor the frequency of data transmission failure for display and logging.

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

L. Door Hardware Interface: Coordinate with Division 08 Sections that specify door hardware required to be monitored or controlled by the PACS. The Controllers in this Section shall have electrical characteristics that match the signal and power requirements of door hardware. Integrate door hardware specified in Division 08 Sections to function with the controls and PC-based software and hardware in this Section.

M. References to industry and trade association standards and codes are minimum installation requirement standards.

N. Drawings and other specification sections shall govern in those instances where requirements are greater than those specified in the above standards.

1.10 EQUIPMENT AND MATERIALS

A. Refer to 25 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1

1.11 WARRANTY OF CONSTUCTIN.

A. Warrant PACS work subject to the Article “Warranty of Construction” of FAR clause 52.246-21.

B. Demonstration and training shall be performed prior to system acceptance.

2 PART 2 - PRODUCTS

2.1 GENERAL

A. The security system characteristics listed in this section will serve as a guide in selection of equipment and materials for the PACS. If updated or more suitable versions are available then the Contracting Officer will approve the acceptance of prior to an installation.

B. PACS equipment shall meet or exceed all requirements listed below.

C. A PACS shall consist of one or more of the following components:

1. Physical Access Control System
2. Application Software
3. System Database
4. Surge and Tamper Protection
5. Standard Workstation Hardware (provided by City of Austin)
6. Communications Workstation
7. Controllers (Data Gathering Panel)
8. Secondary Alarm Annunciator
9. Keypads
10. Card Readers
11. Credential Cards
12. Enrollment Center
13. System Sensors and Related Equipment
14. Push Button Switches
15. Interfaces
16. Door and Gate Hardware interface
17. Floor Select Elevator Control
18. Real Time Guard Tour
19. Video and Camera Control
20. Cables
21. Transformers
22. USB Card Scanners

23. Card Printer
24. Card creation software
25. Card Laminate

2.2 SECURITY MANAGEMENT SYSTEM (SMS)

A. Shall allow the configuration of an enrollment and badging, alarm monitoring, administrative, asset management, digital video management, intrusion detection, visitor enrollment, remote access level management, and integrated client workstations or any combination of all or some.

B. Shall be expandable to support an unlimited number of individual module or integrated client workstations. All access control field hardware, including Data Gathering Panels(DGP), shall be connected to all physical access control system workstation (s) on the network.

C. Shall have the ability to compose, file, maintain, update, and print reports for either individuals or the system as follows.

1. Individual reports that consist of an employee's name, office location, phone number or direct extension, and normal hours of operation. The report shall provide a detail listing of the employee's daily events in relation to accessing points within a facility.
2. System reports shall be able to produce information on a daily/weekly/monthly basis for all events, alarms, and any other activity associated with a system user.

D. All reports shall be in a date/time format and all information shall be clearly presented. Shall be designed to allow it to work with any industry standard network protocol and topology listed below:

1. Transmission Control Protocol (TCP)/IP

E. Shall provide full interface and control of the PACS to include the following subsystems within the PACS:

1. Card Management
2. Identity and Access Management
3. Personal Identity Verification

F. Shall have the following features or compatibilities:

1. The ability to be operated locally or remotely via a LAN, WAN, internet, or intranet.
2. Event and Alarm Monitoring
3. Database Partitioning
4. Ability to fully integrate with all other security sub-systems
5. Alternate and Extended Shunt by Door
6. Escort Management

7. N-man Rule and Occupancy Restrictions
8. Personnel Import
9. Windows Server 2003, Windows 7
10. Field-Level Audit Trail
11. Cardholder Access Events

2.3 APPLICATION SOFTWARE

A. System Software: Based on Windows 7 central-station and workstation operating system and application software. Software shall have the following features:

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

SPEC WRITER NOTE: Retain paragraph below if a single point failure in the Central Station is unacceptable

B. Peer Computer Control Software: Shall detect a failure of a central computer, and shall cause the other central computer to assume control of all system functions without interruption of operation. Drivers shall be provided in both central computers to support this mode of operation.

SPEC WRITER NOTE: DTS links may be included with perimeter protection systems

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

1. Resides at the Central Station, workstations, and Controllers as required to perform specified functions.
2. Operate and manage peripheral devices.
3. Manage files for disk I/O, including creating, deleting, and copying files; and automatically maintain a directory of all files, including size and location of each sequential and random-ordered record.
4. Import custom icons into graphics views to represent alarms and I/O devices.

5. Globally link I/O so that any I/O can link to any other I/O within the same Location, without requiring interaction with the host PC. This operation shall be at the Controller.
6. Globally code I/O links so that any access-granted event can link to any I/O with the same Location without requiring interaction with the host PC. This operation shall be at the Controller.
7. Messages from PC to Controllers and Controllers to Controllers shall be on a polled network that utilizes check summing and acknowledgment of each message. Communication shall be automatically verified, buffered, and retransmitted if message is not acknowledged.
8. Selectable poll frequency and message time-out settings shall handle bandwidth and latency issues for TCP/IP, RF, and other PC-to-Controller communications methods by changing the polling frequency and the amount of time the system waits for a response.
9. Automatic and encrypted backups for database and history backups shall be automatically stored at centralized servers/workstations and.
10. Operator audit trail for recording and reporting all changes made to database and system software.

D. Controller Software:

1. Controllers shall operate as an autonomous intelligent processing unit. Controllers shall make decisions about physical access control, alarm monitoring, linking functions, and door locking schedules for its operation, independent of other system components. Controllers shall be part of a fully distributed processing control network. The portion of the database associated with a Controller and consisting of parameters, constraints, and the latest value or status of points connected to that Controller, shall be maintained in the SMS Server (s) and a copy maintained in the Controller.
2. Functions: The following functions shall be fully implemented and operational within each Controller:
    a. Monitoring inputs.
    b. Controlling outputs.
    c. Automatically reporting alarms to the Central Station.
    d. Reporting of sensor and output status to Central Station on request.
    e. Maintaining real time, automatically updated by the Central Station at least once a day.
    f. Communicating with the Central Station.
    g. Executing Controller resident programs.
    h. Diagnosing.
    i. Downloading and uploading data to and from the Central Station.
3. Controller Operations at a Location:

   a. Location: Up to [64Controllers connected to the communications network. Globally operating I/O linking and anti-passback functions between Controllers within the same Location without central-station or workstation intervention. Linking and anti-passback shall remain fully functional within the same Location even when the Central Station or workstations are off line.

   b. In the event of communications failure between the SMS Server (s) and a Location, there shall be no degradation in operations at the Controllers at that Location. The Controllers at each Location shall be connected to a memory buffer with a capacity to store up to 10,000 events; there shall be no loss of transactions in system history files until the buffer overflows. The Controllers at each Locations shall retain a copy of data from the SMS Servers so that access controls continue to operate.

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

4. Individual Controller Operation:

   a. Controllers shall transmit alarms, status changes, and other data to the Central Station and/or SMS Servers when communications circuits are operable. If communications are not available, Controllers shall function in a stand-alone mode and operational data, including the status and alarm data normally transmitted to the Central Station, shall be stored for later transmission to the Central Station.

   b. Card-reader ports of a Controller shall be custom configurable for at least [120] <Insert number> different card-reader or keypad formats. Multiple reader or keypad formats may be used simultaneously at different Controllers or within the same Controller.

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

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

   e. Initial Startup: When Controllers are brought on-line, database parameters shall be automatically downloaded to them. After initial download is completed, only database changes shall be downloaded to each Controller.

   f. Failure Mode: On failure for any reason, Controllers shall perform an orderly shutdown and force Controller outputs to a predetermined failure mode state, consistent with the failure modes shown and the associated control device.

   g. Startup After Power Failure: After power is restored, startup software shall initiate self-test diagnostic routines, after which Controllers shall resume normal operation.

   h. Startup After Controller Failure: On failure, if the database and application software are no longer resident, Controllers shall not restart, but shall remain in the failure mode until repaired. If database and application programs are resident, Controllers shall immediately resume operation. If not, software shall be restored automatically from the Central Station.

5. Communications Monitoring:
    a. System shall monitor and report status of communications links [TCP/IP communication status] of each Location.
    b. Communication status window shall display which Controllers are currently communicating, a total count of missed polls since midnight, and which Controller last missed a poll.
    c. Communication status window shall show the type of CPU, the type of I/O board, and the amount of RAM memory for each Controller.
6. Operating systems shall include a real-time clock function that maintains seconds, minutes, hours, day, date, and month. The real-time clock shall be automatically synchronized with the Central Station at least once a day to plus or minus 10 seconds. The time synchronization shall be automatic, without operator action and without requiring system shutdown.

E. PC-to-Controller Communications:
    1. Central-station or workstation communications shall use the following:
        a. TCP/IP LAN network interface cards.
    2. TCP/IP network interface card shall have an option to set the poll frequency and message response time-out settings.
    3. PC-to-Controller and Controller-to-Controller communications shall use a polled-communication protocol that checksum and acknowledges each message. All communications shall be verified and buffered and retransmitted if not acknowledged.

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

G. Controller-to-Controller Communications:
    1. Controller-to-Controller Communications: RS-485, 4-wire, point-to-point, regenerative (repeater) communications network methodology.
    2. RS-485 communications signal shall be regenerated at each Controller.

H. Database Downloads:

1. All data transmissions from SMS Servers, Central Stations, or PCs to a Location, and between Controllers at a Location, shall include a complete database checksum to check the integrity of the transmission. If the data checksum does not match, a full data download shall be automatically retransmitted.
2. If a Controller is reset for any reason, it shall automatically request and receive a database download from the SMS Server. The download shall restore data stored at the Controller to their normal working state and shall take place with no operator intervention.

I. Operator Interface:

1. Inputs in system shall have two icon representations, one for the normal state and one for the abnormal state.
2. When viewing and controlling inputs, displayed icons shall automatically change to the proper icon to display the current system state in real time. Icons shall also display the input's state, whether armed or bypassed, and if the input is in the armed or bypassed state due to a time zone or a manual command.
3. Outputs in system shall have two icon representations, one for the secure (locked) state and one for the open (unlocked) state.
4. Icons displaying status of the I/O points shall be constantly updated to show their current real-time condition without prompting by the operator.
5. The operator shall be able to scroll the list of I/Os and press the appropriate toolbar button, or right click, to command the system to perform the desired function.
6. Graphic maps or drawings containing inputs, outputs, and override groups shall include the following:
    a. Database to import and store full-color maps or drawings and allow for input, output, and override group icons to be placed on maps.
    b. Maps to provide real-time display animation and allow for control of points assigned to them.
    c. System to allow inputs, outputs, and override groups to be placed on different maps.
    d. Software to allow changing the order or priority in which maps will be displayed.
7. Override Groups Containing I/Os:
    a. System shall incorporate override groups that provide the operator with the status and control over user-defined "sets" of I/Os with a single icon.
    b. Icon shall change automatically to show the live summary status of points in that group.
    c. Override group icon shall provide a method to manually control or set to time zone points in the group.

        d. Override group icon shall allow the expanding of the group to show icons representing the live status for each point in the group, individual control over each point, and the ability to compress the individual icons back into one summary icon.

    8. Schedule Overrides of I/Os and Override Groups:

        a. To accommodate temporary schedule changes that do not fall within the holiday parameters, the operator shall have the ability to override schedules individually for each input, output, or override group.

        b. Each schedule shall be composed of a minimum of two dates with separate times for each date.

        c. The first time and date shall be assigned the override state that the point shall advance to, when the time and date become current.

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

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

J. Operator Access Control:

    1. Control operator access to system controls through password-protected operator levels. System operators and managers with appropriate password clearances shall be able to change operator levels for operators.

    2. Three successive attempts by an operator to execute functions beyond their defined level during a 24-hour period shall initiate a software tamper alarm.

    3. A minimum of [32] <Insert number> passwords shall be available with the system software. System shall display the operator's name or initials in the console's first field. System shall print the operator's name or initials, action, date, and time on the system printer at login and logoff.

    4. The password shall not be displayed or printed.

    5. Each password shall be definable and assignable for the following:

        a. Commands usable.

        b. Access to system software.

        c. Access to application software.

        d. Individual zones that are to be accessed.

        e. Access to database.

K. Operator Commands:

1. Command Input: Plain-language words and acronyms shall allow operators to use the system without extensive training or data-processing backgrounds. System prompts shall be a word, a phrase, or an acronym.
2. Command inputs shall be acknowledged and processing shall start in not less than [1] <Insert number> second(s).
3. Tasks that are executed by operator's commands shall include the following:
    a. Acknowledge Alarms: Used to acknowledge that the operator has observed the alarm message.
    b. Place Zone in Access: Used to remotely disable intrusion alarm circuits emanating from a specific zone. System shall be structured so that console operator cannot disable tamper circuits.
    c. Place Zone in Secure: Used to remotely activate intrusion alarm circuits emanating from a specific zone.
    d. System Test: Allows the operator to initiate a system-wide operational test.
    e. Zone Test: Allows the operator to initiate an operational test for a specific zone.
    f. Print reports.
    g. Change Operator: Used for changing operators.
    h. Security Lighting Controls: Allows the operator to remotely turn on/off security lights.
    i. Display Graphics: Used to display any graphic displays implemented in the system. Graphic displays shall be completed within 20 seconds from time of operator command.
    j. Run system tests.
    k. Generate and format reports.
    l. Request help with the system operation.
        1) Include in main menus.
        2) Provide unique, descriptive, context-sensitive help for selections and functions with the press of one function key.
        3) Provide navigation to specific topic from within the first help window.
        4) Help shall be accessible outside the applications program.
    m. Entry-Control Commands:
        1) Lock (secure) or unlock (open) each controlled entry and exit up to four times a day through time-zone programming.
        2) Arm or disarm each monitored input up to four times a day through time-zone programming.

        3) Enable or disable readers or keypads up to twice a day through time-zone programming.

        4) Enable or disable cards or codes up to four times per day per entry point through access-level programming.

    n. Command Input Errors: Show operator input assistance when a command cannot be executed because of operator input errors. Assistance screen shall use plain-language words and phrases to explain why the command cannot be executed. Error responses that require an operator to look up a code in a manual or other document are not acceptable. Conditions causing operator assistance messages include the following:

        1) Command entered is incorrect or incomplete.

        2) Operator is restricted from using that command.

        3) Command addresses a point that is disabled or out of service.

        4) Command addresses a point that does not exist.

        5) Command is outside the system's capacity.

L. Alarms:

1. System Setup:

    a. Assign manual and automatic responses to incoming point status change or alarms.

    b. Automatically respond to input with a link to other inputs, outputs, operator-response plans, unique sound with use of WAV files, and maps or images that graphically represent the point location.

    c. 60-character message field for each alarm.

    d. Operator-response-action messages shall allow message length of at least 65,000 characters, with database storage capacity of up to 32,000 messages. Setup shall assign messages to [access point] [zone] [sensor]<other alarm originating device>.

    e. Secondary messages shall be assignable by the operator for printing to provide further information and shall be editable by the operator.

    f. Allow 25 secondary messages with a field of 4 lines of 60 characters each.

    g. Store the most recent 1000 alarms for recall by the operator using the report generator.

2. Software Tamper:

    a. Annunciate a tamper alarm when unauthorized changes to system database files are attempted. Three consecutive unsuccessful attempts to log onto system shall generate a software tamper alarm.

    b. Annunciate a software tamper alarm when an operator or other individual makes three consecutive unsuccessful attempts to invoke functions beyond their authorization level.

        c. Maintain a transcript file of the last 5000 commands entered at the each Central Station to serve as an audit trail. System shall not allow write access to system transcript files by any person, regardless of their authorization level.

        d. Allow only acknowledgment of software tamper alarms.

    3. Read access to system transcript files shall be reserved for operators with the highest password authorization level available in system.

    4. Animated Response Graphics: Highlight alarms with flashing icons on graphic maps; display and constantly update the current status of alarm inputs and outputs in real time through animated icons.

    5. Multimedia Alarm Annunciation: WAV files to be associated with alarm events for audio annunciation or instructions.

    6. Alarm Handling: Each input may be configured so that an alarm cannot be cleared unless it has returned to normal, with options of requiring the operator to enter a comment about disposition of alarm. Allow operator to silence alarm sound when alarm is acknowledged.

    7. Alarm Automation Interface: High-level interface to Central Station alarm automation software systems. Allows input alarms to be passed to and handled by automation systems in same manner as burglar alarms, using an RS-232 ASCII interface.

    8. CCTV Alarm Interface: Allow commands to be sent to Video Monitoring systems during alarms (or input change of state) through serial ports.

    9. Camera Control: Provides operator ability to select and control cameras from graphic maps.

M. Alarm Monitoring: Monitor sensors, Controllers, and DTS circuits and notify operators of an alarm condition. Display higher-priority alarms first and, within alarm priorities, display the oldest unacknowledged alarm first. Operator acknowledgment of one alarm shall not be considered acknowledgment of other alarms nor shall it inhibit reporting of subsequent alarms.

    1. Displayed alarm data shall include type of alarm, location of alarm, and secondary alarm messages.

    2. Printed alarm data shall include type of alarm, location of alarm, date and time (to nearest second) of occurrence, and operator responses.

    3. Maps shall automatically display the alarm condition for each input assigned to that map, if that option is selected for that input location.

    4. Alarms initiate a status of "pending" and require the following two handling steps by operators:

        a. First Operator Step: "Acknowledged." This action shall silence sounds associated with the alarm. The alarm remains in the system "Acknowledged" but "Un-Resolved."

        b. Second Operator Step: Operators enter the resolution or operator comment, giving the disposition of the alarm event. The alarm shall then clear.

5. Each workstation shall display the total pending alarms and total unresolved alarms.
6. Each alarm point shall be programmable to disallow the resolution of alarms until the alarm point has returned to its normal state.
7. Alarms shall transmit to Central Station in real time, except for allowing connection time for dial-up locations.
8. Alarms shall be displayed and managed from a minimum of four different windows.
    a. Input Status Window: Overlay status icon with a large red blinking icon. Selecting the icon will acknowledge the alarm.
    b. History Log Transaction Window: Display name, time, and date in red text. Selecting red text will acknowledge the alarm.
    c. Alarm Log Transaction Window: Display name, time, and date in red. Selecting red text will acknowledge the alarm.
    d. Graphic Map Display: Display a steady colored icon representing each alarm input location. Change icon to flashing red when the alarm occurs. Change icon from flashing red to steady red when the alarm is acknowledged.
9. Once an alarm is acknowledged, the operator shall be prompted to enter comments about the nature of the alarm and actions taken. Operator's comments may be manually entered or selected from a programmed predefined list, or a combination of both.
10. For locations where there are regular alarm occurrences, provide programmed comments. Selecting that comment shall clear the alarm.
11. The time and name of the operator who acknowledged and resolved the alarm shall be recorded in the database.
12. Identical alarms from same alarm point shall be acknowledged at same time the operator acknowledges the first alarm. Identical alarms shall be resolved when the first alarm is resolved.
13. Alarm functions shall have priority over downloading, retrieving, and updating database from workstations and Controllers.
14. When a reader-controlled output (relay) is opened, the corresponding alarm point shall be automatically bypassed.

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

O. System test software enables operators to initiate a test of the entire system or of a particular portion of the system.

1. Test Report: The results of each test shall be stored for future display or printout. The report shall document the operational status of system components.

P. Report Generator Software: Include commands to generate reports for displaying, printing, and storing on disk and tape. Reports shall be stored by type, date, and time. Report printing shall be the lowest priority activity. Report generation mode shall be operator selectable but set up initially as periodic, automatic, or on request. Include time and date printed and the name of operator generating the report. Report formats may be configured by operators.

1. Automatic Printing: Setup shall specify, modify, or inhibit the report to be generated; the time the initial report is to be generated; the time interval between reports; the end of period; and the default printer.
2. Printing on Requests: An operator may request a printout of any report.
3. Alarm Reports: Reporting shall be automatic as initially set up. Include alarms recorded by system over the selected time and information about the type of alarm [(such as door alarm, intrusion alarm, tamper alarm, etc.)] <Insert alarm types>, the type of sensor, the location, the time, and the action taken.
4. Access and Secure Reports: Document zones placed in access, the time placed in access, and the time placed in secure mode.
5. Custom Reports: Reports tailored to exact requirements of who, what, when, and where. As an option, custom report formats may be stored for future printing.
6. Automatic History Reports: Named, saved, and scheduled for automatic generation.
7. Cardholder Reports: Include data, or selected parts of the data, as well as the ability to be sorted by name, card number, imprinted number, or by any of the user-defined fields.
8. Cardholder by Reader Reports: Based on who has access to a specific reader or group of readers by selecting the readers from a list.
9. Cardholder by Access-Level Reports: Display everyone that has been assigned to the specified access level.
10. Who Is In (Muster) Report:
    a. Emergency Muster Report: One click operation on toolbar launches report.
    b. Cardholder Report. Contain a count of persons that are "In" at a selected Location and a count with detailed listing of name, date, and time of last use, sorted by the last reader used or by the group assignment.
11. Panel Labels Reports: Printout of control-panel field documentation including the actual location of equipment, programming parameters, and wiring identification. Maintain system installation data within system database so that they are available on-site at all times.

12. Activity and Alarm On-Line Printing: Activity printers for use at workstations; prints all events or alarms only.

13. History Reports: Custom reports that allows the operator to select any date, time, event type, device, output, input, operator, Location, name, or cardholder to be included or excluded from the report.

    a. Initially store history on the hard disk of the host PC.

    b. Permit viewing of the history on workstations or print history to any system printer.

    c. The report shall be definable by a range of dates and times with the ability to have a daily start and stop time over a given date range.

    d. Each report shall depict the date, time, event type, event description, device, or I/O name, cardholder group assignment, and cardholder name or code number.

    e. Each line of a printed report shall be numbered to ensure that the integrity of the report has not been compromised.

    f. Total number of lines of the report shall be given at the end of the report. If the report is run for a single event such as "Alarms," the total shall reflect how many alarms occurred during that period.

14. Reports shall have the following four options:

    a. View on screen.

    b. Print to system printer. Include automatic print spooling and "Print To" options if more than one printer is connected to system.

    c. "Save to File" with full path statement.

    d. System shall have the ability to produce a report indicating status of system inputs and outputs or of inputs and outputs that are abnormal, out of time zone, manually overridden, not reporting, or in alarm.

Q. Anti-Passback:

1. System shall have global and local anti-passback features, selectable by Location. System shall support hard and soft anti-passback.

2. Hard Anti-Passback: Once a credential holder is granted access through a reader with one type of designation (IN or OUT), the credential holder may not pass through that type of reader designation until the credential holder passes though a reader of opposite designation.

3. Soft Anti-Passback: Should a violation of the proper IN or OUT sequence occur, access shall be granted, but a unique alarm shall be transmitted to the control station, reporting the credential holder and the door involved in the violation. A separate report may be run on this event.

4. Timed Anti-Passback: A Controller capability that prevents an access code from being used twice at the same device (door) within a user-defined amount of time.
5. Provide four separate zones per Location that can operate without requiring interaction with the host PC (done at Controller). Each reader shall be assignable to one or all four anti-passback zones. In addition, each anti-passback reader can be further designated as "Hard," "Soft," or "Timed" in each of the four anti-passback zones. The four anti-passback zones shall operate independently.
6. The anti-passback schemes shall be definable for each individual door.
7. The Master Access Level shall override anti-passback.
8. System shall have the ability to forgive (or reset) an individual credential holder or the entire credential holder population anti-passback status to a neutral status.

R. Visitor Assignment:

1. Provide for and allow an operator to be restricted to only working with visitors. The visitor badging subsystem shall assign credentials and enroll visitors. Allow only access levels that have been designated as approved for visitors.
2. Provide an automated log of visitor name, time and doors accessed, and whom visitor contacted.
3. Allow a visitor designation to be assigned to a credential holder.
4. PACS shall be able to restrict the access levels that may be assigned to credentials that are issued to visitors.
5. Allow operator to recall visitors' credential holder file, once a visitor is enrolled in the system.
6. The operator may designate any reader as one that deactivates the credential after use at that reader. The history log shall show the return of the credential.
7. System shall have the ability to use the visitor designation in searches and reports. Reports shall be able to print all or any visitor activity.

S. Entry-Control Enrollment Software: Database management functions that allow operators to add, delete, and modify access data as needed.

1. The enrollment station shall not have alarm response or acknowledgment functions.
2. Provide multiple, password-protected access levels. Database management and modification functions shall require a higher operator access level than personnel enrollment functions.
3. The program shall provide means to disable the enrollment station when it is unattended to prevent unauthorized use.

4. The program shall provide a method to enter personnel identifying information into the entry-control database files through enrollment stations. In the case of personnel identity verification subsystems, this shall include biometric data. Allow entry of personnel identifying information into the system database using menu selections and data fields. The data field names shall be customized during setup to suit user and site needs. Personnel identity verification subsystems selected for use with the system shall fully support the enrollment function and shall be compatible with the entry-control database files.
5. Personnel Search Engine: A report generator with capabilities such as search by last name, first name, group, or any predetermined user-defined data field; by codes not used in definable number of days; by skills; or by seven other methods.
6. Multiple Deactivate Dates for Cards: User-defined fields to be configured as additional stop dates to deactivate any cards assigned to the cardholder.
7. Batch card printing.
8. Default card data can be programmed to speed data entry for sites where most card data are similar.
9. Enhanced ACSII File Import Utility: Allows the importing of cardholder data and images.
10. SPEC WRITER NOTE: Retain paragraph below if visitor badge return is part of system
11. Card Expire Function: Allows readers to be configured to deactivate cards when a card is used at selected devices.

T. System Redundancy & High Availability: The system shall provide multiple levels of communications redundancy and failover for all PACS hosted controllers, digital video recorders, and client workstations. The PACS shall be capable of automatically re-routing communications to alternate computers across the system without operator intervention.

SPEC WRITER NOTE: Retain paragraph X.1 or X.2 as applicable for the project.

1. PACS system configuration shall provide at a minimum the following redundancy and failover capability:
   a. The PACS shall provide communications redundancy and failover for network-attached devices. Each network attached device shall have one or more alternative communication sever(s) that can provide hosting in case of primary communications server failure.
   b. In case of primary communications server failure, the system shall automatically re-route network-attached devices to their designated backup communications servers to allow continuous system operations without loss of alarm and event transaction processing during failover.

    c. Network-attached devices which transition to backup communications servers, shall be able to be redirected back to their default primary servers, once the primary communications servers have been restored.

2. PACS system configuration with multiple regional application/ database servers shall provide at a minimum the following redundancy and failover capability:
    a. The PACS shall support the same level of communications redundancy and failover for network-attached devices per regional application/database server, allowable to span across regional application/database servers in the event of a regional application/database server failure.
    b. In case of a regional application/database server failure, client workstations shall be able to failover to their designated backup regional application/database server to allow continuous system operations.
    c. In case of a regional application/database server failure, upon server restoration, the ISMS shall automatically update and synchronize the regional application/database server.
    d. Client workstations which transition to a backup regional application/database server, shall be able to be redirected back to their default regional application/database server, once the regional application/database server functions have been restored.

2.4 SURGE AND TAMPER PROTECTION

A. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor-entry connection to components.
    1. Minimum Protection for Power Connections 120 V and More: Auxiliary panel suppressors complying with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits."
    2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Connections: Comply with requirements in Division 26 Section "Transient-Voltage Suppression for Low-Voltage Electrical Power Circuits" as recommended by manufacturer for type of line being protected.

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

2.5 CONTROLLERS

A. Controllers: Intelligent peripheral control unit, complying with UL 294, that stores time, date, valid codes, access levels, and similar data downloaded from the Central Station or workstation for controlling its operation.

B. Subject to compliance with requirements in this Article, manufacturers may use multipurpose Controllers.

C. Battery Backup: Sealed, lead acid; sized to provide run time during a power outage of 90 minutes, complying with UL 924.

D. Alarm Annunciation Controller:

  1. The Controller shall automatically restore communication within 10 seconds after an interruption with the field device network.

    a. Inputs: Monitor dry contacts for changes of state that reflect alarm conditions. Provides at least eight alarm inputs, which are suitable for wiring as normally open or normally closed contacts for alarm conditions.

    b. Alarm-Line Supervision:

      1) Supervise the alarm lines by monitoring each circuit for changes or disturbances in the signalby monitoring for abnormal open, grounded, or shorted conditions using dc change measurements. System shall initiate an alarm in response to an abnormal current, which is a dc change of [5] [10] percent or more for longer than 500 ms.

      2) Transmit alarm-line-supervision alarm to the Central Station during the next interrogation cycle after the abnormal current condition.

    c. Outputs: Managed by Central Station software.

  2. Auxiliary Equipment Power: A [GFI] service outlet inside the Controller enclosure.

E. Entry-Control Controller:

  1. Function: Provide local entry-control functions including one- and two-way communications with access-control devices such as card readers, keypads, biometric personal identity verification devices, door strikes, magnetic latches, gate and door operators, and exit push-buttons.

    a. Operate as a stand-alone portal Controller using the downloaded database during periods of communication loss between the Controller and the field-device network.

    b. Accept information generated by the entry-control devices; automatically process this information to determine valid identification of the individual present at the portal:

      1) On authentication of the credentials or information presented, check privileges of the identified individual, allowing only those actions granted as privileges.

        2) Privileges shall include, but not be limited to, time of day control, day of week control, group control, and visitor escort control.

    c. Maintain a record of date, time, and Locationfor each transaction. A transaction is defined as any successful or unsuccessful attempt to gain access through a controlled portal by the presentation of credentials or other identifying information.

2. Inputs:

    a. Data from entry-control devices; use this input to change modes between access and secure.

    b. Database downloads and updates from the Central Station and/or SMS Server that include enrollment and privilege information.

3. Outputs:

    a. Indicate success or failure of attempts to use entry-control devices and make comparisons of presented information with stored identification information.

    b. Grant or deny entry by sending control signals to portal-control devices, and mask intrusion alarm annunciation from sensors stimulated by authorized entries.

    c. Transmit transaction records to the Central Station.

    d. Door Prop/Door Ajar Alarm: If a portal is held open for longer than than the programmed period of time, issue alarm message, and sound alarm, if required.

4. Data Line Problems: For periods of loss of communications with Central Station, or when data transmission is degraded and generating continuous checksum errors, the Controller shall continue to control entry by accepting identifying information, making authentication decisions, checking privileges, and controlling portal-control devices.

    a. Store up to [1000] <Insert number> transactions during periods of communication loss between the Controller and access-control devices for subsequent upload to the Central Station on restoration of communication.

5. Backup Battery: Premium, valve-regulated, recombinant-sealed, lead-calcium battery; spill proof; with a full 1-year warranty [and a pro rata 19-year warranty]. With single-stage, constant-voltage-current, limited battery charger, comply with battery manufacturer's written instructions for battery terminal voltage and charging current recommendations for maximum battery life.

    a. Backup Power Supply Capacity: [5] [90] minutes of battery supply. Submit battery and charger calculations.

6. Power Monitoring: Provide manual dynamic battery load test, initiated and monitored at the control center; with automatic disconnection of the Controller when battery voltage drops below Controller limits. Report by using local Controller-mounted LEDs and by

communicating status to Central Station. Indicate normal power on and battery charger on trickle charge. Indicate and report the following:

   a. Trouble Alarm: Normal power off load assumed by battery.
   b. Trouble Alarm: Low battery.
   c. Alarm: Power off.

2.6 CARD READERS

A. Power: Card reader shall be powered from its associated Controller, including its standby power source.

B. Response Time: Card reader shall respond to passage requests by generating a signal that is sent to the Controller. Response time shall be [800]<insert number>ms or less, from the time the card reader finishes reading the credential card until a response signal is generated.

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

   1. Indoors, controlled environment.
   2. Indoors, uncontrolled environment.
   3. Outdoors, with weather-sealed enclosuresn, and with built-in heaters or other cold-weather equipment to extend the operating temperature range as needed for operation at the site.

D. Display: LED or other type of visual indicator display shall provide visualand audible status indications and user prompts. Indicate power on/off, whether user passage requests have been accepted or rejected, and whether the door is locked or unlocked.

E. Shall be utilized for controlling the locking hardware on a door and allows for reporting back to the main control panel with the time/date/location the door was accessed, the name of the person accessing the point of entry, and its location.

F. Will be fully programmable and addressable, locally and remotely, and hardwired to the system.

G. Shall be individually home run to the main panel.

H. Shall be installed in a manner that they comply with:

   1. The Uniform Federal Accessibility Standards (UFAS)
   2. The Americans with Disabilities Act (ADA)
   3. The ADA Standards for Accessible Design

I. Shall support a variety of card readers that must encompass a wide functional range. The PACS may combine any of the card readers described below for installations requiring multiple types of card reader capability (i.e., card only, card and/or PIN, card and/or biometrics, card and/or pin and/or biometrics, supervised inputs, etc.). The reader output can be Wiegand, RS-22, 485 or TCP/IP.

J. Shall contain read head electronics, and a sender to encode digital door control signals.

K. LED’s shall be utilized to indicate card reader status and access status (allow/decline).

L. Shall be able to support a user defined downloadable off-line mode of operation (e.g. locked, unlocked), which will go in effect during loss of communication with the main control panel.

M. Shall provide audible feedback to indicate access granted/denied decisions. Upon a card swipe, two audible tones or beeps shall indicate access granted and three tones or beeps shall indicate access denied. All keypad buttons shall provide tactile and audible feedback.

N. Shall have a minimum of two programmable inputs and two programmable outputs.

O. All card readers that utilize keypad controls along with a reader and shall meet the following specifications:

   1. Entry control keypads shall use a unique combination of alphanumeric and other symbols as an identifier. Keypads shall contain an integral alphanumeric/special symbols keyboard with symbols arranged in ascending ASCII code ordinal sequence. Communications protocol shall be compatible with the local processor.

P. Shall include a Light Emitting Diode (LED) or other type of visual indicator display and provide visual or visual and audible status indications and user prompts. The display shall indicate power on/off, and whether user passage requests have been accepted or rejected. The design of the keypad display or keypad enclosure shall limit the maximum horizontal and vertical viewing angles of the keypad. The maximum horizontal viewing angle shall be plus and minus five (5) degrees or less off a vertical plane perpendicular to the plane of the face of the keypad display. The maximum vertical viewing angle shall be plus and minus 15 degrees or less off a horizontal plane perpendicular to the plane of the face of the keypad display.

   1. Shall respond to passage requests by generating a signal to the local processor. The response time shall be 800 milliseconds or less from the time the last alphanumeric symbol is entered until a response signal is generated.
   2. Shall be powered from the source as designed and shall not dissipate more than 150 Watts.
   3. Shall be suitable for surface, semi-flush, pedestal, or weatherproof mounting as required.
   4. Shall provide a means for users to indicate a duress situation by entering a special code.

2.7 KEYPADS

A. Designed for use with unique combinations of alphanumeric and other symbols as an Identifier. Keys of keypads shall contain an integral alphanumeric/special symbol keyboard with symbols arranged in [ascending ASCII-code ordinal sequence. Communications protocol shall be compatible with Controller.

   1. Keypad display or enclosure shall limit viewing angles of the keypad as follows:

    a. Maximum Horizontal Viewing Angle: 5 degrees or less off in either direction of a vertical plane perpendicular to the plane of the face of the keypad display.
    b. Maximum Vertical Viewing Angle: 15 degrees or less off in either direction of a horizontal plane perpendicular to the plane of the face of the keypad display.
2. Duress Codes: Provide duress situation indication by entering a special code.

2.8 CREDENTIAL CARDS

A. Printed Credential Cards shall be HID iClass /35 Bit Corp 1000 without embedded indala chips, unless otherwise specified as with indala chips.

B. Clamshell Credential Cards shall be HID 2080PGSNV iClass clamshell cards.

2.9 SYSTEM SENSORS AND RELATED EQUIPMENT

A. The PACS (Physical Access Control System) and related Equipment provided by the Contractor shall meet or exceed the following performer specifications:

B. Request to Exit Detectors:

1. Passive Infrared Request to Exit Motion Detector (REX PIR) (1) The Contractor shall provide a surface mounted motion detector to signal the physical access control system request to exit input. The motion detector shall be a passive infrared sensor designed for wall or ceiling mounting 2134 to 4572 mm (7 to 15 ft) height. The detector shall provide two (2) form “C” (SPDT) relays rated one (1) Amp. @ 30 VDC for DC resistive loads. The detectors relays shall be user adjustable with a latch time from 1-60 seconds. The detector shall also include a selectable relay reset mode to follow the timer or absence of motion. The detection pattern shall be adjustable plus or minus fourteen (± 14) degrees. The detector shall operate on 12 VDC with approximately 26 mA continuous current draw. The detector shall have an externally visible activation LED. The motion detector shall measure approximately 38 mm H x 158 mm W x 38 mm D (1.5 x 6.25 x 1.5 in). The detector shall be immune to radio frequency interference. The detector shall not activate or set-up on critical frequencies in the range 26 to 950 Megahertz using a 50 watt transmitter located 30.5 cm (1 ft) from the unit or attached wiring. The detector shall be available on gray or black enclosures. The color of the housing shall be coordinated with the surrounding surface.

C. Guard tour stations:

1. Guard tour station (s) shall be single gang brushed steel plate flush mounted in a single gang box. The switch shall be a normally open momentary keyed switch.

D. Delayed Egress (DE)

1. General: - The delay egress locking hardware shall provide a method to secure emergency exits and provide an approved delayed emergency exit method. The package shall be Underwriters Laboratories listed as a delay egress-locking device. The delay egress device

shall be available to support configurations with both rated and non-rated fire doors. The delay egress device shall comply with Life Safety Codes (NFPA-101, BOCA) as it applies to special locking arrangements for delay egress locks. Unless specifically identified as a non-fire rated opening, all doors shall be equipped with fire rated door hardware. The Contractor shall be responsible for providing all equipment and installation to provide a fully functioning system. Need to amend to use crashbars type mechanical release switches.

2. The delay-locking device shall include all of the following features:
   a. Delay Egress Mode
      1) The delayed egress device shall be a SDC 101V Series Exit Check with wall mounted control module. Upon activation of an approved panic bar the delay locking device shall begin a delay sequence of 30 seconds; a flush mounted wall LED panel adjacent to the door will indicate initiation of the countdown time. During the 30 second delay period, a local sounding device shall annunciate a tone activation of the delay cycle and verbal exit instructions. At the end of the delay cycle the locking device shall unlock and allow free egress. The reset of the local sounding device shall be user definable and include options to select either local sound until silenced by reset or local sounder silenced upon opening of the door. Unless otherwise indicated the local delay sounder shall be silenced upon opening of the door. The SDC's device trigger output shall be connected to the SMS DGP alarm panel for pre-activation warning. The contractor shall specify the bond sensor option when ordering the delayed egress hardware; this output shall be wired to the SMS DGP to activate an alarm if the door does not lock. Use of reset panel not top mounted device.
      2) Delayed egress doors will have bond sensors.
      3) Delayed egress activation shall also trigger Video Monitoring call –up.
      4) The delayed egress shall be resettable through the SMS.
3. The Contractor shall provide a Master Open Switch for all the facility's delayed egress hardware, with protective cover and permanent labeling in the Unit Control Room. When the switch is pressed all delayed egress or evacuation doors shall unlock and generate an alarm at the security console monitor showing and recording time and date of when the switch was pressed.
4. Each individual delayed egress door shall have the ability to unlock through a manual action on the SMS.
5. Unless otherwise indicated, the Contractor shall provide all of the above reset methods for each door. All signs will meet the latest ADA requirements.
6. Signs - The delay egress package shall be provided with a warning sign complying with local code requirements. The warning sign shall be attached to the interior side of the controlled door. The sign shall be located on the interior side of the door above and within 304 mm (12 in) of the panic bar. The sign shall read:

EMERGENCY EXIT.

PUSH UNTIL

ALARM SOUNDS

DOOR CAN BE OPENED,

IN 30 SECONDS.

a. Signs shall be coordinated and comply with the building's existing sign specifications. Signs shall include grade 2 Braille.

b. Signs shall meet the current ADA requirements.

c. In instances of code and specification conflicts, the life safety code requirement shall prevail.

d. The Division 10 Contractor shall provide samples for approval with their submittal package.

7. Physical Access Control Interface

   a. The delay egress device shall be capable of interface with card access control systems.

   b. The system shall include a bypass feature that is activated via a dry contact relay output from the physical access control system. This bypass shall allow authorized personnel to pass through the controlled portal without creating an alarm condition or activating the delay egress cycle. The bypass shall include internal electronic shunts or door switches to prevent activation (re-arming) until the door returns to the closed position. An unused access event shall not cause a false alarm and shall automatically rearm the delay egress lock upon expiration of the programmed shunt time. The delay egress physical access control interface shall support extended periods of automated and/or manual lock and unlock cycles.

E. Crash Bar:

1. Emergency Exit with Alarm (Panic):

   a. Entry control portals shall include panic bar emergency exit hardware as designed.

   b. Panic bar emergency exit hardware shall provide an alarm shunt signal to the PACS and SMS.

   c. The panic bar shall include a conspicuous warning sign with one (1) inch (2.5 cm) high, red lettering notifying personnel that an alarm will be annunciated if the panic bar is operated.

   d. Operation of the panic bar hardware shall generate an intrusion alarm that reports to both the SMS and Intrusion Detection System.

   e. The panic bar shall utilize a fully mechanical connection only and shall not depend upon electric power for operation.

f. The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt manually by either pressing the panic bar or with a key by-pass. Refer to Section 2.2.I.9 for key-bypass specifications.

g. Normal Exit:

  1) Entry control portals shall include panic bar non-emergency exit hardware as designed.

  2) Panic bar non-emergency exit hardware shall be monitored by and report to the SMS.

  3) Operation of the panic bar hardware shall not generate a locally audible or an intrusion alarm within the IDS.

  4) When exiting, the panic bar shall depend upon a mechanical connection only. The exterior, non-secure side of the door shall be provided with an electrified thumb latch or lever to provide access after the credential I.D. authentication by the SMS.

  5) The panic bar shall be compatible with mortise or rim mount door hardware and shall operate by retracting the bolt manually by either pressing the panic bar or with a key by-pass. Refer to Section 2.2.I.9 for key-bypass specifications. The strikes/bolts shall include a micro switch to indicate to the system when the bolt is not engaged or the strike mechanism is unlocked. The signal switches shall report a forced entry to the system in the event the door is left open or accessed without the identification credentials.

F. Door Status Indicators:

1. Shall monitor and report door status to the SMS.

2. Door Position Sensor:

   a. Shall provide an open or closed indication for all doors operated on the PACS and report directly to the SMS.

   b. Shall also provide alarm input to the Intrusion Detection System for all doors operated by the PACS and all other doors that require monitoring by the intrusion detection system.

   c. The switch shall monitor door position and report to the intrusion detection system. For doors with electromagnetic locks a magnetic bonding sensor (MBS) can be used

   d. Switches for doors not operated by the PACS shall report directly to the IDS.

   e. Shall be surface or flush mounted and wide gap with the ability to operate at a maximum distance of up to 2” (5 cm).

2.10 PUSH BUTTON SWITCHES

A. Push-Button Switches: Momentary-contact back-lighted push buttons, with stainless-steel switch enclosures.

  1. Electrical Ratings:

    a. Minimum continuous current rating of [10] <Insert number> A at 120 V ac or [5] <Insert number> A at 240-V ac.

    b. Contacts that will make 720 VA at [60] <Insert number> A and that will break at 720 VA at [10] <Insert number> A.

  2. Enclosures: Flush or surface mounting. Push buttons shall be suitable for flush mounting in the switch enclosures.

  3. Enclosures shall additionally be suitable for installation in the following locations:

    a. Indoors, controlled environment.

    b. Indoors, uncontrolled environment.

    c. Outdoors.

  4. Power: Push-button switches shall be powered from their associated Controller, using dc control.

2.11 PORTAL CONTROL DEVICES

A. Shall be used to assist the PACS.

B. Such devices shall:

  1. Provide a means of monitoring the doors status.

  2. Allow for exiting a space via either a push button, request to exit, or panic/crash bar.

  3. Provide a means of override to the PACS via a keypad or key bypass.

  4. Assist door operations utilizing automatic openers and closures.

C. Provide a secondary means of access to a space via a keypad.

D. Shall be connected to and monitored by the main PACS panel.

E. Shall be installed in a manner that they comply with:

  1. The Uniform Federal Accessibility Standards (UFAS)

  2. The Americans with Disabilities Act (ADA)

  3. The ADA Standards for Accessible Design

F. Shall provide a secondary means of physical access control within a secure area.

G. Push-Button Switches:

1. Shall be momentary contact, back lighted push buttons, and stainless steel switch enclosures for each push button as shown. Buttons are to be utilized for secondary means of releasing a locking mechanism.
    a. In an area where a push button is being utilized for remote access of the locking device then no more than two (2) buttons shall operate one door from within one secure space. Buttons will not be wired in series with one other.
    b. In an area where locally stationed guards control entry to multiple secure points via remote switches. An interface board shall be designed and constructed for only the amount of buttons it shall house. These buttons shall be flush mounted and clearly labeled for ease of use. All buttons shall be connected to the PACS and SMS system for monitoring purposes.

H. Entry Control Devices:

1. Shall be hardwired to the PACS main control panel and operated by either a card reader via a relay on the main control panel.
2. Shall be fail-safe in the event of power failure to the PACS system.
3. Shall operate at 24 VDC, with the exception of turnstiles and be powered by a separate power supply dedicated to the door control system. Each power supply shall be rated to operate a minimum of two doors simultaneously without error to the system or overload the power supply unit.
4. Electric Strikes/Bolts: Shall be:
    a. Made of heavy-duty construction and tamper resistant design.
    b. Tested to over one million cycles.
    c. Rated for a minimum of 1000 lbs. holding strength.
    d. Utilize an actuating solenoid for the strike/bolt. The solenoid shall move from fully open to fully closed position and back in not more than 500 milliseconds and be rated for continuous duty.
    e. Utilize a signal switch that will indicate to the system if the strike/bolt is not engaged or is unlocked when it should be secured.
    f. Flush mounted within the door frame.
5. Electric Mortise Locks: Shall be installed within the door and an electric transfer hinge shall be utilized to allow the wires to be transferred from the door frame to the lock. If utilized with a double door then the lock shall be installed inside the active leaf. Electric Mortise Locks shall:
    a. These locks shall be provided and installed by the Division 8 “DOOR HARDWARE” Contractor, unless otherwise specified.

b. Have integrated Request to Exit switch for doors receiving physical access control devices.

c. Provide integration of the Electric Mortise Locks with the PACS for:

   1) Lock Power

   2) Request to Exit switch.

6. Electromagnetic Locks:

   a. These locks shall be without mechanical linkage utilizing no moving parts, and securing the door to its frame solely on electromagnetic force.

   b. Shall be comprised of two pieces, the mag-lock and the door plate. The electromagnetic locks shall be surface mounted to the door frame and the door plate shall be surface mounted to the door.

   c. Ensure a diode is installed in line with the DC voltage supplying power to the unit in order to prevent back-check on the system when the electromagnetic lock is powered.

   d. Shall utilize a magnetic bonding sensor (MBS) to monitor the door status and report that status to the SMS.

   e. Electromagnetic locks shall meet the following minimum technical characteristics:

Operating Voltage		24 VDC
Current Draw		.5A
Holding Force	Swing Doors	675 kg (1500 lbs)
	Sliding Doors	225 kg (500 lbs)

   f. In high-security areas, use balanced magnetic switch sensors, not magnetic bonding sensors.

7. Turnstiles:

   a. Shall operate at 110 VAC, 60 Hz or 220 VAC, 50 Hz supplied from a dedicated circuit breaker on a security power panel. This device does not require a back-up power source.

   b. Shall be utilized as a means of monitoring and controlling access in a lobby.

   c. Shall meet the following minimum requirements:

      1) Provide either an audible or visual confirmation that access has been granted to a cleared individual.

      2) Provide an audible alarm in the event a non-cleared individual is attempting to gain access.

        3) Interface with the SMS and utilize a card reader for accessing and exiting a facility, and provide a recorded event of personnel accessing these points.

        4) Have a built-in step-down transformer to provide power to a card reader unit.

        5) Have built-in signal wiring chassis to allow for plug and play capabilities with the PACS.

        6) Have the ability to detect tailgating within one quarter on an inch to prevent

8. Vehicle Gate Operator: Interface electrical operation of gate with controls of this Section. Vehicle gate operators shall be connected, monitored, and controlled, by the security access Controllers. Vehicle gate and accessories are specified in Division 32 Section "Chain Link Fences and Gates."

2.12 INTERFACES

A. Video Monitoring System Interface

1. An Ethernet interface associated driver and controller shall be provided for connection of the SMS Central Computer to the Video Monitoring Video Monitoring alarm interface and switcher. The interface shall provide alarm data to the Video Monitoring Alarm interface for automatic camera call-up, if required in scope of work. If required, the Security Contractor shall be responsible for programming the command strings into the SMS Server.

B. Intercom System Interface

1. The Video Monitoring call-up from intercom stations shall be through the intercom unit via serial or Ethernetcommunications interface to the SMS system.

    a. Application Software

        1) Provides the interface between the Alarm Annunciation System and Operator; all sensors, local processors and data links, drive displays, report alarms, and report generation.

        2) Software is categorized as System Software and Application Software. System Software must consist of software to support set-up, operation, hard drive back-ups and maintenance processor. Application Software must consist of software to provide the completion of Physical Access Control System.

C. Power Supplies:

1. Shall be UL rated and able to adequately power the specified number of entry control devices on a continuous base without failure.

2.13 FLOOR SELECT ELEVATOR CONTROL

A. Access Control system shall be capable of interfacing with Elevator system to allow/deny access to elevators.

   1. System shall be capable of providing full elevator security and control through dedicated Controllers without relying on the control-station host PC for elevator control decisions.
   2. Access-control system shall enable and disable car calls on each floor and floor select buttons in each elevator car, restricting passengers' access to the floors where they have been given access.
   3. System setup shall, through programming, automatically secure and unsecure each floor select button of a car individually by time and day. Each floor select button within a car shall be separately controlled so that some floors may be secure while others remain unsecure.
   4. When a floor select button is secure, it shall require the passenger to use his/her access code and have access to that floor before the floor select button will operate. The passenger's credential shall determine which car call and floor select buttons are to be enabled, restricting access to floors unless authorized by system's access code database. Floor select button shall be enabled only in the car where the credential holder is the passenger.

B. PACS shall record which call button is pressed, along with credential and time information.

   1. System Controller shall record elevator access data.
   2. The Controller shall reset all additional call buttons that may have been enabled by the user's credential.
   3. The floor select elevator control shall allow for manual override either individually by floor or by cab as a group from a workstation PC.

2.14 REAL TIME GUARD TOUR

A. Guard tour module shall provide the ability to plan, track, and route tours. Module shall input an alarm during tour if guard fails to make a station. Tours can be programmed for sequential or random tour-station order.

   1. Guard tour setup shall define specific routes or tours for the guard to take, with time restrictions in which to reach every predefined tour station.
   2. Guard tour activity shall be automatically logged to the Central Station, and to the SMS server.
   3. If the guard is early or late to a tour station, a unique alarm per station shall appear at the Central Station to indicate the time and station.
   4. Guard tour setup shall allow the tours to be executed sequentially or in a random order with an overall time limit set for the entire tour instead of individual times for each tour station.

5. Setup shall allow recording of predefined responses that will display for the operator at the control station should a "Failed to Check-in" alarm occur.

B. A tour station is a physical location a guard shall reach and perform an action indicating that the guard has arrived. This action, performed at the tour station, shall be 1 of 13 different events with any combination of station types within the same tour. A tour station shall be one of the following event types:

1. Access Granted.
2. Access Denied Code.
3. Access Denied Card plus PIN.
4. Access Denied Time Zone.
5. Access Denied Level.
6. Access Denied Facility.
7. Access Denied Code Timer.
8. Access Denied Anti-Passback.
9. Access Granted Passback Violation.
10. Alarm.
11. Restored.
12. Input Normal.
13. Input Abnormal.

C. Guard tour and other system features shall operate simultaneously with no interference.

D. Guard Tour Module Capacity: 999 possible guard tour definitions with each tour having up to 99 tour stations. System shall allow all 999 tours to be running at same time.

2.15 VIDEO AND CAMERA CONTROL

A. Control station or designated workstation displays live video from a Video Monitoring source.

1. Control Buttons: On the display window, with separate control buttons to represent Left, Right, Up, Down, Zoom In, Zoom Out, Scan, and a minimum of two custom command auxiliary controls.
2. Provide on-screen icons to represent different types of cameras, with ability to import custom icons. Provide option for display of icons on graphic maps to represent their physical location.
3. Provide the alarm-handling window with a command button that will display the camera associated with the alarm point.

B. Display mouse-selectable icons representing each camera source, to select source to be displayed. For Video Monitoring sources that are connected to a video switcher, control station shall automatically send control commands to display the requested camera when the camera icon is selected.

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

3 PART 3 - EXECUTION

3.1 GENERAL

A. The Contractor shall install all system components and appurtenances in accordance with the manufacturers' instructions, ANSI C2, and shall furnish all necessary interconnections, services, and adjustments required for a complete and operable system as specified. Control signals, communications, and data transmission lines grounding shall be installed as necessary to preclude ground loops, noise, and surges from affecting system operation. Equipment, materials, installation, workmanship, inspection, and testing shall be in accordance with manufacturers' recommendations and as modified herein.

B. Consult the manufacturers' installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc., before beginning system installation. Refer to the Riser/Connection diagram for all schematic system installation/termination/wiring data.

C. All equipment shall be attached to walls and ceiling/floor assemblies and shall be held firmly in place (e.g., sensors shall not be supported solely by suspended ceilings). Fasteners and supports shall be adequate to support the required load.

D. Coordinate with Division 27 //Owner// to locate, connect and provision data network connections and configurations.

3.2 CURRENT SITE CONDITIONS

A. The Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions which will affect performance of the system to the Owner in a report as defined in paragraph Group II Technical Data Package. The Contractor shall not take any corrective action without written permission from the Owner.

3.3 EXAMINATION

A. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

B. Examine roughing-in for LAN and control cable conduit systems to PCs, Controllers, card readers, and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.4 PREPARATION

A. Comply with EIA/TIA-606, "Administration Standard for the Telecommunications Infrastructure of Commercial Buildings."

B. Obtain detailed Project planning forms from manufacturer of access-control system; develop custom forms to suit Project. Fill in all data available from Project plans and specifications and publish as Project planning documents for review and approval.

    1. Record setup data for control station and workstations.
    2. For each Location, record setup of Controller features and access requirements.
    3. Propose start and stop times for time zones and holidays, and match up access levels for doors.
    4. Set up groups, linking, and list inputs and outputs for each Controller.
    5. Assign action message names and compose messages.
    6. Set up alarms. Establish interlocks between alarms, intruder detection, and video surveillance features.
    7. Prepare and install alarm graphic maps.
    8. Develop user-defined fields.
    9. Develop screen layout formats.
    10. Propose setups for guard tours and key control.
    11. Discuss badge layout options; design badges.
    12. Complete system diagnostics and operation verification.
    13. Prepare a specific plan for system testing, startup, and demonstration.
    14. Develop acceptance test concept and, on approval, develop specifics of the test.
    15. Develop cable and asset management system details; input data from construction documents. Include system schematics and Technical Drawings.

C. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software

D. For integration purposes, the PACS shall be integrated where appropriate with the following associated security subsystems:

   1. CCTV:

      a. Provide 24 hour coverage of all entry points to the perimeter and agency buildings, and all emergency exits utilizing a fixed color camera.

      b. Be able to monitor, control and record cameras on a 24 hours basis.

      c. Be programmed automatically call up a camera when an access point is put into an alarm state.

      d. For additional PACS system requirements as they relate to the CCTV, refer to Section 28 23 00, VIDEO SURVEILLANCE.

   2. IDS:

      a. Be able monitor door control sensors.

      b. Be able to monitor and control the IDS on a 24 hours basis.

      c. Be programmed to go into an alarm state when an IDS device is put into an alarm state, and notify the operator via an audible and visual alarm.

   3. For additional PACS system requirements as they relate to the IDS, refer to Section 28 16 11, INTRUSION DETECTION SYSTEM.

   4. Security Access Detection:

      a. For additional PACS system requirements as they relate to the Security Access Detection, refer to Section 28 13 53, SECURITY ACCESS DETECTION.

   5. EPPS:

      a. Be programmed to go into an alarm state when an emergency call box or duress alarm/panic device is activated, and notify the Physical Access Control System and Database Management of an alarm event.

      b. For additional PACS requirements as they relate to the EPPS, refer to Section 28 26 00, ELECTRONIC PERSONAL PROTECTION SYSTEM.

E. Integration with these security subsystems shall be achieved by computer programming or the direct hardwiring of the systems.

F. For programming purposes, refer to the manufacturers requirements for correct system operations. Ensure computers being utilized for system integration meet or exceed the minimum system requirements outlined on the systems software packages.

G. The Contractor shall visit the site and verify that site conditions are in agreement with the design package. The Contractor shall report all changes to the site or conditions that will affect performance of the system. The Contractor shall not take any corrective action without written permission from the City of Austin.

H. Existing Equipment:

    1. The Contractor shall connect to and utilize existing door equipment, control signal transmission lines, and devices as outlined in the design package. Door equipment and signal lines that are usable in their original configuration without modification may be reused with Contracting Officer approval.
    2. The Contractor shall perform a field survey, including testing and inspection of all existing door equipment and signal lines intended to be incorporated into the PACS, and furnish a report to the Contracting Officer as part of the site survey report. For those items considered nonfunctioning, provide (with the report) specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency. As part of the report, the Contractor shall include a schedule for connection to all existing equipment.
    3. The Contractor shall make written requests and obtain approval prior to disconnecting any signal lines and equipment, and creating equipment downtime. Such work shall proceed only after receiving Contracting Officer approval of these requests. If any device fails after the Contractor has commenced work on that device, signal or control line, the Contractor shall diagnose the failure and perform any necessary corrections to the equipment.
    4. The Contractor shall be held responsible for repair costs due to Contractor negligence, abuse, or improper installation of equipment.
    5. The Contracting Officer shall be provided a full list of all equipment that is to be removed or replaced by the Contractor, to include description and serial/manufacturer numbers where possible. The Contractor shall dispose of all equipment that has been removed or replaced based upon approval of the Contracting Officer after reviewing the equipment removal list. In all areas where equipment is removed or replaced the Contractor shall repair those areas to match the current existing conditions.

I. Enclosure Penetrations: All enclosure penetrations shall be from the bottom of the enclosure unless the system design requires penetrations from other directions. Penetrations of interior enclosures involving transitions of conduit from interior to exterior, and all penetrations on exterior enclosures shall be sealed with rubber silicone sealant to preclude the entry of water and will comply with Division 07 84 00, Firestopping. The conduit riser shall terminate in a hot-dipped galvanized metal cable terminator. The terminator shall be filled with an approved sealant as recommended by the cable manufacturer and in such a manner that the cable is not damaged.

J. Cold Galvanizing: All field welds and brazing on factory galvanized boxes, enclosures, and conduits shall be coated with a cold galvanized paint containing at least 95 percent zinc by weight.

K. Control Panels:

    1. Connect power and signal lines to the controller.

    2. Program the panel as outlined by the design and per the manufacturer’s programming guidelines.

L. SMS:

    1. Coordinate with the City of Austin agency’s IT personnel to place the computer on the local LAN or Intranet and provide the security system protection levels required to insure only authorized City of Austin personnel have access to the system.
    2. Program and set-up the SMS to ensure it is fully operational.

M. Card Readers:

    1. Connect all signal inputs and outputs as shown and specified.
    2. Terminate input signals as required.
    3. Program and address the reader as per the design package.
    4. Readers shall be surface or flushed mounted and all appropriate hardware shall be provided to ensure the unit is installed in an enclosed conduit system.

N. Portal Control Devices:

    1. Install all signal input and output cables as well as all power cables.
    2. Devices shall be surface or flush mounted as per the design package.
    3. Program all devices and ensure they are working.

O. Door Status Indicators:

    1. Install all signal input and output cables as well as all power cables.
    2. RTE’s shall be surface mounted and angled in a manner that they cannot be compromised from the non-secure side of a windowed door, or allow for easy release of the locking device from a distance no greater than 6 feet from the base of the door.
    3. Door position sensors shall be surface or flush mounted and wide gap with the ability to operate at a maximum distance of up to 2” (5 cm).

P. Entry Control Devices:

    1. Install all signal input and power cables.
    2. Strikes and bolts shall be mounted within the door frame.
    3. Mortise locks shall be mounted within the door and an electric transfer hinge shall be utilized to transfer the wire from within the door frame to the mortise lock inside the door.
    4. Electromagnetic locks shall be installed with the mag-lock mounted to the door frame and the metal plate mounted to the door.

Q. System Start-Up:

1. The Contractor shall not apply power to the PACS until the following items have been completed:
    a. PACS equipment items and have been set up in accordance with manufacturer's instructions.
    b. A visual inspection of the PACS has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.
    c. System wiring has been tested and verified as correctly connected as indicated.
    d. All system grounding and transient protection systems have been verified as installed and connected as indicated.
    e. Power supplies to be connected to the PACS have been verified as the correct voltage, phasing, and frequency as indicated.
    f. System power wiring is in compliance with NEC standards for wire gauge and color-coding, or is in compliance with the local Authority Having Jurisdiction (AHJ) for electrical codes.
2. Satisfaction of the above requirements shall not relieve the Contractor of responsibility for incorrect installation, defective equipment items, or collateral damage as a result of Contractor work efforts.
3. The City of Austin will observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the City. Provide a minimum of 7 days prior notice.

R. Supplemental Contractor Quality Control:
    1. The Contractor shall provide the services of technical representatives who are familiar with all components and installation procedures of the installed PACS.
    2. The Contractor will be present on the job site during the preparatory and initial phases of quality control to provide technical assistance.
    3. The Contractor shall also be available on an as needed basis to provide assistance with follow-up phases of quality control.
    4. The Contractor shall participate in the testing and validation of the system and shall provide certification that the system installed is fully operational as all construction document requirements have been fulfilled.

3.5 SYSTEM SOFTWARE

A. Install, configure, and test software and databases for the complete and proper operation of systems involved. Assign software license to Owner.

3.10 FIELD QUALITY CONTROL

A. Perform the following field tests and inspections and prepare test reports:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Use Class 2, bidirectional, Category 5 tester. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA-568-1, "Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA-568-B.
2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.
3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

3.6 COMMISSIONING

A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up, and contractor testing required above and required by the System Readiness Checklist provided by the Commissioning Agent.

B. Components provided under this section of the specification will be tested as part of a larger system. Refer to Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for contractor responsibilities for system commissioning.

3.7 DEMONSTRATION AND TRAINING

A. See 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY SYSTEMS, PART 3 – EXECUTION, 3.9 System Training

-----END----

28 13 16 PHYSICAL ACCESS CONTROL DATABASE MANAGEMENT FOR ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0, City of Austin, Texas

January, 2014

1 PART 1 - GENERAL

1.1 DESCRIPTION

A. This section specifies the finishing, installation, connection, testing and certification of a complete and fully operation Physical Access Control Database Management System, hereinafter referred to as the PACMS.

B. This Section includes a Physical Security Access System Database Management consisting of database management software. Requirements for hardware supporting database management are described in Section 28 13 00 PHYSICAL ACCESS CONTROL, Part 2.

1.2 RELATED WORK

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 28 05 00 – COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. Requirements for general requirements that are common to more than one section in Division 28.

C. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

D. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding and bonding.

E. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.

F. Section 28 08 00 - COMMISIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. For requirements for commissioning and systems readiness checklists.

G. Section 28 13 00 - PHYSICAL ACCESS CONTROL SYSTEM. Requirements for physical access control system.

H. Section 28 13 53 - SECURITY ACCESS DETECTION. Requirements for screening of personnel and shipments.

I. Section 28 16 00 - INTRUSION DETECTION SYSTEM (IDS). Requirements for alarm systems.

J. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

K. Section 28 26 00 - ELECTRONIC PERSONAL PROTECTION SYSTEM (EPPS). Requirements for emergency and interior communications.

1.3 QUALITY ASSURANCE

A. See 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY SYSTEMS, PART 1 – GENERAL, 1.4 Quality Assurance

2 PART 2 - PRODUCTS

2.1 SYSTEM DATABASE

A. Database and database management software shall define and modify each point in database using operator commands. Definition shall include parameters and constraints associated with each system device.

B. Database Segmentation:

1. The System shall employ advanced database segmentation functionality. Each segment shall be allowed to have its own unique set of cardholders, hardware, and system parameters including access control field hardware, timezones, access levels, etc. As such, only credentials that are assigned access levels to card readers in a segment need to be downloaded to the Data Gathering Panels in that segment.
2. Cardholders shall be allowed to belong to one segment, many segments, or all segments.
3. The database segmentation functionality shall also provide a capability to object records in the system, where segment System Administrators and Operators can only view, add, modify, delete, and manipulate cardholders, system parameters and access control field hardware that belong to their respective segments.
4. System Administrators and System Operators shall be assigned the segments they are allowed to view and control. System Administrators and System Operators may be assigned to more than one segment and a segment may be assigned to more than one System Administrator and System Operator. A one-to-many relationship shall exist for System Administrators and System Operators with respect to segments. The SYSTEM shall support a minimum of [65,000] <insert number> segments.
5. System Administrators and System Operators shall be allowed to assign or revoke access privileges to cardholders that belong to any segment in the database, but not be allowed to modify, delete or otherwise manipulate cardholder records in segments that the Administrator or Operator does not control.

C. Bi-Directional Data Exchange

1. The System shall also support a one-step download and distribution process of cardholder and security information from the external database to the SMS database, all the way down to the Controller local database. This shall be a guaranteed process, even if the communication path between the SYSTEM database server and the Controller is broken. If the communication path is broken, the data shall be stored in a temporary queue and shall be automatically downloaded once the communication path is restored.

D. Database connectivity:

   1. The SMS database shall support network database connectivity for importing cardholder and card ID data from external systems and/or database applications. The PACS SMS shall facilitate interfacing by providing the following capabilities:
      - a. Real time and batch processing of data over a network connection.
      - b. Insert, update, and delete record information.
      - c. Automatic download of data to control panels (data gathering panels) based on database changes.
      - d. Provide audit trail in the operator history/archive database for all database changes initiated by the interface.

E. Operator Passwords:

   1. Software shall support up to [32,000] <insert number> individual system operators, each with a unique password.
   2. Allow use of Single sign-on (SSO) password.
   3. Passwords shall not be displayed when entered.
   4. Operators shall use a user name and password to log on to system.
      - a. This user name and password is used to access database areas and programs as determined by the associated profile.
   5. Make provision to allow the operator to log off without fully exiting program. User may be logged off but program will remain running while displaying the login window for the next operator.

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

   1. Access authorization shall verify the card or card-and-PIN validation, and the access level (time of day, day of week, date), anti-passback status, and number of uses last.
   2. Use data-entry windows to view, edit, and issue access levels. Access authorization entry management system shall maintain and coordinate all access levels to prevent duplication or the incorrect creation of levels.
   3. Allow assignment of multiple cards/codes to a cardholder.
   4. Allow assignment of at least four access levels for each Location to a cardholder. Each access level may contain any combination of doors.
   5. Each door may be assigned four time zones.
   6. Access codes may be up to 11 digits in length.

7. Software shall allow the grouping of locations so cardholder data can be shared by all locations in the group.
8. Visitor Access: Issue a visitor badge, without assigning that person a card or code, for data tracking or photo ID purposes.
9. Cardholder Tracing: Allow for selection of cardholder for tracing. Make a special audible and visual annunciation at control station when a selected card or code is used at a designated code reader. Annunciation shall include an automatic display of the cardholder image.
10. Allow option for each cardholder to be given either an unlimited number of uses or a number of uses that regulates the number of times the card can be used before it is automatically deactivated.
11. Provide for cards and codes to be activated and deactivated manually or automatically by date. Provide for multiple deactivate dates to be preprogrammed.

G. Security Access Integration:

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

H. Groups:

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

I. Time Zones:

1. Each zone consists of a start and stop time for 7 days of the week and three holiday schedules. A time zone is assigned to inputs, outputs, or access levels to determine when an input shall automatically arm or disarm, when an output automatically opens or secures, or when access authorization assigned to an access level will be denied or granted.
2. Up to four time zones may be assigned to inputs and outputs to allow up to four arm or disarm periods per day or four lock or unlock periods per day; up to three holiday override schedules may be assigned to a time zone.
3. Data-entry window shall display a dynamically linked bar graph showing active and inactive times for each day and holiday, as start and stop times are entered or edited.
4. System shall have the capacity for [2048] <Insert number> time zones for each Location.

A. Holidays:

1. Three different holiday schedules may be assigned to a time zone. Holiday schedule consists of date in format MM/DD/YYYY and a description. When the holiday date matches the current date of the time zone, the holiday schedule replaces the time zone schedule for that 24-hour period.
2. System shall have the capacity for [32,000] <Insert number> holidays.
3. Three separate holiday schedules may be applied to a time zone.
4. Holidays have an option to be designated as occurring on the designated date each year. These holidays remain in system and will not be purged.
5. Holidays not designated to occur each year shall be automatically purged from database after the date expires.

B. Access Levels:

1. System shall allow for the creation at least [32,000] <Insert number> access levels.
2. System shall allow for access to be restricted to any area by reader and by time. Access levels shall determine when and where an Identifier is authorized.
3. System shall be able to create multiple door and time zone combinations under same access level so that an Identifier may be valid during different time periods at different readers even if the readers are on the same Controller.

C. User-Defined Fields:

1. System shall provide a minimum of 99 user-defined fields, each with up to 50 characters, for specific information about each credential holder.
2. System shall accommodate a title for each field; field length shall be 20 characters.
3. A "Required" option may be applied to each user-defined field that, when selected, forces the operator to enter data in the user-defined field before the credential can be saved.
4. A "Unique" option may be applied to each user-defined field that, when selected, will not allow duplicate data from different credential holders to be entered.
5. Data format option may be assigned to each user-defined field that will require the data to be entered with certain character types in specific spots in the field entry window.
6. A user-defined field, if selected, will define the field as a deactivate date. The selection shall automatically cause the data to be formatted with the windows MM/DD/YYYY date format. The credential of the holder will be deactivated on that date.
7. A search function shall allow any one user-defined field or combination of user-defined fields to be searched to find the appropriate cardholder. The search function shall include search for a character string.
8. System shall have the ability to print cardholders based on and organized by the user-defined fields.

A. Code Tracing:

1. System shall perform code tracing selectable by cardholder and by reader.
2. Any code may be designated as a "traced code" with no limit to how many codes can be traced.

3. Any reader may be designated as a "trace reader" with no limit to which or how many readers can be used for code tracing.
4. When a traced code is used at a trace reader, the access-granted message that usually appears on the monitor window of the Central Station shall be highlighted with a different color than regular messages. A short singular beep shall occur at the same time the highlighted message is displayed on the window.
5. The traced cardholder image (if image exists) shall appear on workstations when used at a trace reader.

B. Database and File Replication:

1. The Security Management System shall be capable of supporting database and file replication using [Microsoft SQL Server Replication Services and Microsoft File Replication Services] for providing distributed database replication across multiple PACS application servers allowing for system expansion and delivering N tiers of server redundancy.
2. Database and file replication shall not require any proprietary database or file replication software.

3 PART 3 - EXECUTION

3.1 INSTALLATION

SPEC WRITER NOTE: Delete and/or amend this all paragraphs and sub-paragraphs to apply to only the equipment and devices that are being installed.

A. System installation shall be in accordance with manufacturer and related documents and references, for each type of security subsystem designed, engineered and installed.

B. All software shall be installed per the design package and the manufacturer’s installation specifications.

3.2 TESTING AND TRAINING

All testing and training shall be compliant with the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.

Perform testing and system certification as outlined in section 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY.

A. The software shall be entered into the SMS computer systems and debugged. The Contractor shall be responsible for documenting and entering the initial database into the system. The Contractor shall provide the necessary blank forms with instructions to fill in all the required data information that will make up the database. The database shall then be reviewed by the Contractor and entered into the system. Prior to full operation, a complete demonstration of the computer real time functions shall be performed. A printed validation log shall be provided as proof of operation for each software application package. In addition, a point utilization report shall be furnished listing each point, the associated programs utilizing that point as an input or output and the programs which that point initiates.

B. Upon satisfactory on line operation of the system software, the entire installation including all subsystems shall be inspected. The Contractor shall perform all tests, furnish all test equipment and consumable supplies necessary and perform any work as required to establish performance levels for the system in accordance with the specifications. Each device shall be tested as a working component of the completed system. All system controls shall be inspected for proper operation and response.

C. Tests shall demonstrate the response time and display format of each different type of input sensor and output control device. Response time shall be measured with the system functioning at full capacity. Computer operation shall be tested with the complete data file.

D. The Contractor shall provide a competent trainer who has extensive experience on the installed systems and in delivering training to provide the instruction. As an alternative, the Contractor may propose the use of factory training personnel and coordinate the number of personnel to be trained.

3.3 MAINTENANCE

A. The Contractor shall offer a Support Agreement (SSA) in order for Technical Support Specialists to reactively troubleshoot system problems.

B. As part of the agreement, 5x9 telephone support (Standard and Enhanced SSA) will be provided to the Contractor by Certified Technicians. An option of 7x24 Standby telephone support (Enhanced SSA) shall be offered.

C. As part of the agreement, Flashable and Non-Flashable (Chips) firmware and documentation shall be provided.

D. As part of the agreement, access to Security Management System (SMS)software patches and software release updates shall be provided.

E. The Support Agreement shall cover the current version of the SMS software release one full version back, and associated controller hardware.

-----END----

28 13 53 SECURITY ACCESS DETECTION FOR ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0, City of Austin, Texas

January, 2014

1 PART 1 - GENERAL

1.1 DESCRIPTION

A. Provide and install a complete Detection and Screening System, hereinafter referred to as the Security Access Detection as specified in this section.

1.2 RELATED WORK

SPECS WRITER NOTE: Delete any item or paragraph not applicable in the section and renumber the paragraphs.

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

C. Section 10 14 00 - SIGNAGE. Requirements for labeling and signs.

D. Section 28 05 00 - COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. For general requirements that are common to more than one section in Division 28.

E. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

F. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

G. Section 28 05 28.33 - CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.

H. Section 28 08 00 - COMMISIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS. For commissioning requirements, systems readiness checklists, and training.

I. Section 28 13 00 - PHYSICAL ACCESS CONTROL SYSTEMS (PACS). Requirements for physical access control integration.

J. Section 28 13 16 - ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT. Requirements for control and operation of all security systems.

K. Section 28 16 00 - INTRUSION DETECTION SYSTEM. Requirements for alarm systems.

L. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

M. Section 28 26 00 - ELECTRONIC PERSONAL PROTECTION SYSTEM (EPPS). Requirements for emergency and interior communications.

1.3 QUALITY ASSURANCE

A. Refer to 28 05 00 COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY, Part 1

1.4 APPLICABLE PUBLICATIONS

The publications listed below (including amendments, addenda, revisions, supplement, and errata) form a part of this specification to the extent referenced. The publications are referenced in the text by the basic designation only.

A. American Society for Testing and Materials (ASTM)

C1238-97 (R03) Standard Guide for Installation of Walk-Through Metal Detectors

B. Department of Justice American Disability Act (ADA)

C. Institute of Electrical and Electronics Engineers (IEEE):

C95.1-05 Standards for Safety Levels with Respect to Human Exposure in Radio Frequency Electromagnetic Fields

D. National Fire Protection Association (NFPA):

70-11 Article 780-National Electrical Code

E. National Institute of Justice (NIJ)

0601.02-03 Standards for Walk-Through Metal Detectors for use in Weapons Detection

0602.02-03 Hand-Held Metal Detectors for Use in Concealed Weapon and Contraband Detection

F. National Electrical Manufactures Association (NEMA)

250-08 Enclosures for Electrical Equipment (1000 Volts Maximum)

G. Occupational and Safety Health Administration (OSHA):

29 CFR 1910.97 Nonionizing radiation

H. Security Industry Association (SIA):

AG-01 Security CAD Symbols Standards

I. Underwriters Laboratories, Inc. (UL):

187-98 Standard for X-ray Equipment

464-03 Audible Signal Appliances

J. United States Department of Commerce:

Special Pub 500-101 Care and Handling of Computer Magnetic Storage Media

K. Uniform Federal Accessibility Standards (UFAS), 1984

L. Architectural Barriers Act (ABA), 1968

2 PART 2 - PRODUCTS

2.1 GENERAL

Spec Note: Delete and/or amend this all paragraphs and sub-paragraphs to apply to only the equipment and devices that are being installed.

A. All specifications listed within this section are the minimum requirements to be met to ensure a working Security Access Detection is in place.

B. Detection Sensor subsystems shall consist of sensors capable of:

  1. Locating and identifying prohibited, threatening, contraband materials and items the system is designed to detect and protect against being brought into a facility.

  2. Sensors shall be adjustable to maximize capabilities based on environmental and security requirement changes.

C. Annunciation: Shall contain one (1) or more indicator lamps, alphanumeric displays that provide status information about a circuit or condition of the operating units. Walk-Through or conveyer pass through units must provide a uniform two-digit error code to identify different types of system failures.

D. Audible Signal Device: Shall consist of audible sound for alarms, supervisory, and trouble signals and shall be distinctive.

E. Assessment: Shall consist of electronic devices required to visually and audibly verify the validity and functionality of Security Access Detection. Assessment also includes providing indication of tampering, fail-safe, low battery, and power losses.

F. Alarm Reporting: Shall consist of electronic devices to annunciate Security Access Detection information to at least two (2) separate locations. The alarms shall maintain the capability to respond with local and remote visible and audible signals upon activation of detection sensors. The alarms should have the capability of a silent mode only alerting personnel using the system.

G. Power Supply: Security Access Detection shall be capable of continuous operation and include a battery backup module capable of 12 hrs. of backup use. All non-portable systems shall operate on 100-240 VAC. Hand-Held Security Access Detection (Metal and Explosive Detectors) shall have the capability to operate on rechargeable batteries.

2.2 WALK-THROUGH METAL DETECTORS:

A. Shall meet NIJ Standard 0601.02 and be able to detect and locate guns, knives, and other flat and rod-shaped objects regardless of orientation.

B. All electronics shall be modular in design for easy plug-in and replacement. The Detector shall use multiple coil circuits with dual alarm lights to indicate which side of the individual the detected item is located.

C. Shall be capable of self-diagnostics and conduct self-test of all systems to automatically identify failures or problems with components as displayed on the control unit liquid crystal display (LCD). The detection unit shall not require re-calibration each time the system is turned off and back on.

D. Shall provide for full body coverage: coverage on the left, center, right, front, and back of the body from head to floor, providing uniform detection.

E. Shall include individual zones that are adjustable for customization of detection characteristics and/or compensation for metallic environmental challenges.

F. Shall have the capability to detect and discriminate signals from two (2) or more detectable items located in close proximity that may be detected as only one (1).

G. Shall include adjustable legs to provide for accurate leveling on uneven floors.

H. Major components include:

1. Walk-through portal/passage way
2. Control Unit
3. Test Unit

I. Technical Characteristics:

Operating Temperatures	-4°F (-20°C) to 158°F (70°C) 95% humidity non-condensing
Power Supply Unit	Fully automatic input 100 to 240 VAC 50 or 60 Hz – five (5) watts Uninterrupted Power supply (UPS) Battery Backup (12 hours)
Construction	Minimum 3/32 in. (2.381mm) aluminum in strength and weather resistant
Opening Sizes	Interior Width: 30 in. (762mm) Interior Height: 80 in.(2.032 meters)
Programmable	Capable of 16 independent programs settings for zones and sensitivity
Sensitivity Boost	Three (3) levels at ankle level
Detection Sensors	Multi-dimensional coil 33 distinct pin-point zones – customizable
Sensitivity Levels	200
Interference Protection	Faraday shielding
Alarms	Audible and light-emitting diode (LED) Visual
Testing Device	Simulate size, shape, and composition of threat objects meet FAA testing requirements
Traffic Flow Indicators	LED Lights

Infrared Sensor	Traffic control and counter

J. Control Unit: Shall consist of the components to constantly monitor, input settings, and verify inputs of sensors.

1. The control unit is to be attached to the exit side of the scanner or shall be able to be detached and operational from up to 50 feet (ft.) (15.24 meters)(m) from detector.
2. The control unit will consist of a multiple functional electronic digital keypad/touchpad. The keypad/touchpad requires human/machine interface (HMI) with numerical or function keys that can activate, deactivate, observe or change sensitivity and detector settings using secure codes.
3. The Control Unit shall be programmed to be self-prompting for input.
4. The LCD display shall be large, easily seen, backlit with alpha-numeric display that reports in words to regulate, control and provide self-prompt functions of the control unit.
5. Control Unit Technical Characteristics:

Display	LCD
Connection to Unit	Wired with extension of 50 ft. (15.24m) for remote use
Touchpad Controls	Operate, Off, Counter, Volume, +/-, Program and Access
Displays	LED bar-graphs for detection sensitivity Alarm lights Functionality Program in operation Errors Traffic Count Alarm activations Alarm Percentages
Tamper alarm	10 seconds after access of touchpad
Access Control	Dual-level access codes for: Operators Supervisors

K. Control Unit Interface:

1. The system shall include an interface module for network transmission of data and remote monitoring of system at the Physical Access Control System and Database Management.
2. Integration with the Physical Access Control System and Database Management shall allow for control, real time monitoring and diagnostics capabilities.
3. Control Unit Interface Technical Characteristics:

Display	LCD (laptop or Desktop Monitor)
Connection	10-Base T Network
System Capabilities	Monitor up to 4 scanners
Capabilities	Change settings LED bar-graph display Functionality Program in operation Errors Traffic Count Alarm activations Alarm Percentages Technician trouble-shoot
Access Control	Dual-level access codes Operators Supervisory

2.3 HAND-HELD METAL DETECTORS

A. Shall meet NIJ Standard 0602.02 and be rugged in design and water-proof; lightweight to reduce stress of handling; and provide ease of freedom of movement and control.

B. Shall be easily made operational with a one (1) switch operation that does not require any adjustments.

C. Technical Characteristics:

Operating Temperatures	-35°F (-37°C) to 158°F (70°C) 95% humidity non-condensing
Operating Frequency	93 kHz
Audio Frequency	2kHz Warble Earphone capable
Tuning	Automatic
Controls	Power switch On/Off Interference Elimination
LED Alert Lights	Power On, Battery Low, Alarm
Indicators	Silent/Vibrate Audible Speaker

	LED Alert Lights
Power	Standard 9 volt and Nickel-Metal Hydride(NiMH)rechargeable battery
Battery life	60 hours continuous operations
Minimum Detection Capability Distances	Medium Pistol – 9 in. (228.6mm) Large Knife- 5 in. (127mm) Razor Blade- 3 in. (76.2mm) Small foil and jewelry – 1 in.

2.4 X-RAY DETECTORS:

A. Shall be surface mounted, multilayer, fully integrated, high frequency, and solid state using high speed processors.

B. Shall meet NIJ Standards including a Personal Computer (PC) based system that can be networked with other inspection systems and can transmit data.

C. The type of X-ray unit selected shall require consideration of its application and use (i.e., used to screen items through lobby control points versus screening items, which may be larger in size, such as through mail room/shipping and receiving facility areas).

D. The system should provide the capability to send images through a network to a central server PC where the images can be viewed, stored or printed.

E. The conveyer belt system belts should be guaranteed to perform auto tracking for life.

F. All x-ray systems shall be certified to be in full compliance with all international radiation safety requirements and external emissions limits.

G. Technical Characteristics:

X-Ray Generator	Self Contained operating at 90 kilovolts
Controls	Edge sharpening, variable intensity control, zoom, atomic number measurement
Zoom Capability	2X to 32X penetration levels
Discrimination	Organic, inorganic, mixed
Penetration	0.39 in. (10 mm) steel
Resolution capability	Detect #40 AWG
Color Tones	Two (2) million (Multi-Energy Colors)
Conveyer belt weight capabilities	200 lbs. (90 kilograms)
Conveyer belt speed	Controllable – 48 fpm (24 cm/sec)- reversible

Network Capable	Ethernet using TCP/IP

H. Central Processing Unit Technical Characteristics:

Processor	2.4 GHz Intel Pentium IV
Hard Disk Size	40 GB
Memory	256 RAM
Network Card	10/100 Base-T
CD-ROM Drive	10X
Monitor/Video Adapter board	19” (482.6mm)SVGA (1280 x 1044)Flicker Free Flat Screen .28 dot pitch
Floppy Drive	1.44 MB
Ports	2 serial, 1 parallel, USB
Backup	Tape or CDRW

2.5 EXPLOSIVES DETECTORS:

A. Handheld: Provide for a self-contained analytical unit, with on-board computer, printer and touch screen display. The detector shall be easy to operate by non-technical staff/operators:

1. System will use dual vapor and particulate detection without any external carrier gas or radioactive source.
2. Detector shall be a simple push-button automatic operation that displays go/no go results on a LCD display.
3. Explosive Detectors Technical Characteristics:

Power	12 volt direct current (DC) rechargeable 12 volt External battery pack 12 volt AC adapter
Device Controls	Power switch, keypad, automatic vapor/particulate selector, volume control (with optional earphone, and sample switch.
Memory	Store a minimum of 1000 previous readings
Detection	Dual vapor and particulate
Detection Analysis	<20 seconds
Detection Capabilities	Nanogram levels of: C-4, TNT, Dynamite, PETN, Semtex, EGDN, DMNB, RDX, ANFO, Black Powder, Ammonium Nitrate, Urea Nitrate, Nitroglycerine and TATP

B. Desktop:

1. Shall have a built-in networking and communication capability. The device shall easily interface with other screening systems and printer if it is not part of the unit.
2. Shall be self-contained, self-cleaning, self-calibrating, and require no external gas supply.
3. A touch screen display shall be provided that displays both alarm and compound identification information Red flashing light on unit and audible alarm Automatic "Print on Alarm" option.
4. Contractor shall provide collection device for input of data.
5. Technical Characteristics:

Power	90 to 265 volts alternating current (VAC) 50-60 Hz
Technology	Dual- gas chromatography and Ion mobility spectrometer
Power Consumption	Less than 500 watts
Device Controls	Touch screen display Power switch
Operating Modes	Continuous and Single Cycle
Warm up time	< 20 minutes (cold start)
Memory	Store a minimum of 1000 previous readings
Detection	Dual vapor and particulate
Analysis Time	< 20 seconds
Detection Capabilities	Nanogram levels of: 1) Explosives: PETN, RDX,TNT, NG, Dynamite, Semtex, C4 2) Narcotics: Cocaine, Opiates (heroine & morphine), Cannabis marijuana & hashish), Amphetamine-type stimulants amphetamine, ecstasy & methamphetamine.

3 PART 3 - EXECUTION

3.1 GENERAL

Spec Note: Delete and/or amend this all paragraphs and sub-paragraphs to apply to only the equipment and devices that are being installed.

A. System installation shall be in accordance with appropriate NEC, UL, NFPA, Related Work VA specifications, and appropriate installation manual for each type of Security Access Detection.

B. The Security Access Detection system will be designed, engineered, installed, and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the system is a stand alone or a complete network.

C. Components shall be configured with appropriate “service points” to pinpoint system trouble in less than 30 minutes.

D. All Security Access Detection requiring VAC connection will be installed with surge protection and Uninterrupted Power Supply (UPS).

E. Architectural space planning design requirements need to be considered and defined prior to the installation of metal detection, x-ray and explosive detection equipment at main lobby entrance or other security control points. This also applies to the use of x-ray and explosive detectors in mail and shipping/receiving facility areas.

F. The Contractor shall install all system components including Government furnished equipment, and appurtenances in accordance with the manufacturer's instructions and documentation, and shall furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a complete and operable system.

G. Walk-through metal detectors will not be located on floors with high metal content that may interfere with screening without protection between the floor and detector being considered.

H. The Contractor shall provide walk-through metal detectors with the capability for floor mounting (OEM recommended brackets) to increase stability.

3.2 WIRING

A. See Section 28 05 13 CONDUCTORS AND CABLES

3.3 FIELD QUALITY CONTROL

A. See Division 28 05 00 COMMON WORK RESULTS

3.4 ADJUSTING

A. Occupancy Adjustments: When requested within 12 months of date of Substantial Completion, provide on-site assistance in adjusting system to suit actual occupied conditions and to optimize performance of the installed equipment. Tasks shall include, but are not limited to, the following:

   1. Check cable connections.
   2. Check proper operation of detectors.
   3. Recommend changes to walk trough detectors, X-ray machines, and associated equipment to improve Owner' utilization of security access detection system.
   4. Provide a written report of adjustments and recommendations.

B. Adjustment/Alignment/Synchronization: Contractor shall prepare for system activation by following manufacturer’s recommended procedures for adjustment, alignment, programming, or synchronization. Prepare each component in accordance with appropriate provisions of the component’s installation, operations, and maintenance instructions.

3.5 CLEANING

A. Cleaning: Subsequent to installation, clean each system component of dust, dirt, grease, or oil incurred during installation in accordance to manufacture instructions.

3.6 INTEGRATION

A. For integration purposes, the Security Access Detection system shall be integrated with the Physical Access Control System and Database Management via CAT-V cables and where appropriate with CCTV and EPPS. The CCTV Security System will:

  1. Provide full coverage of all lobby entrance screening areas utilizing a fixed color camera.
  2. Record activity on a 24 hours basis.
  3. The CCTV system should have facial recognition software to assist in identifying individuals for current and future purposes.
  4. For additional CCTV system requirements as they relate to the Security Access Detection, refer to Section 28 13 53, SECURITY ACCESS DETECTION.

B. Integration with CCTV and EPPS security subsystems shall be achieved by computer programming or the direct hardwiring of the systems.

C. For programming purposes, refer to the manufacturers requirements for correct system operations. Ensure computer hardware being utilized for system integration meets or exceeds the minimum system requirements as well as systems software requirements.

3.7 EXISTING CONDITIONS

A. The Contractor shall visit the site and verify that site conditions are in agreement/compliance with the design package. The Contractor shall report all changes to the site or conditions that will affect performance of the system to the Contracting Officer in the form of a report. The Contractor shall not take any corrective action without written permission received from the Contracting Officer.

B. Existing Equipment

  1. The Contractor shall connect to and utilize existing equipment, and control signal transmission lines, and devices as outlined in the design package. Equipment and signal lines that are usable in their original configuration without modification may be reused with Contracting Officer approval.
  2. The Contractor shall perform a field survey, including testing and inspection of all existing equipment, power outlets, and signal lines intended to be used by the Security Access Detection, and furnish a report to the Contracting Officer as part of the site survey report. For those items considered nonfunctioning, provide (with the report) specification sheets, or written functional requirements to support the findings and the estimated cost to correct the deficiency. As part of the report, the Contractor shall include a schedule for connection to all existing equipment.
  3. The Contractor shall make written requests and obtain approval prior to disconnecting any signal lines and equipment, and creating equipment downtime. Such work shall proceed only after receiving Contracting Officer approval of these requests. If any device fails after the Contractor has commenced work on that device, signal or control line, the Contractor shall diagnose the failure and perform any necessary corrections to the equipment.

4. The Contractor shall be held responsible for repair costs due to Contractor negligence, abuse, or improper installation of equipment.
5. The Contracting Officer shall provide a full list of all equipment that is to be removed or replaced by the Contractor. The Contractor shall dispose of all equipment that has been removed or replaced. In all areas where equipment is removed or replaced the Contractor shall repair those areas to match the current existing conditions.

3.8 SYSTEM START-UP AND TESTING

A. System Start-Up
   1. The Contractor shall not apply power to any installed Security Access Detection until the following items have been completed:
      a. Security Access Detection equipment items have been set up in accordance with manufacturer's instructions.
      b. A visual inspection of the Security Access Detection system has been conducted to ensure that defective equipment items have not been installed and that there are no loose connections.
      c. System wiring has been tested and verified as correctly connected as indicated.
      d. All system grounding and transient protection systems have been verified as installed and connected as indicated.
      e. Power supplies to be connected to the Security Access Detection system have been verified as the correct voltage, phasing, and frequency as indicated by the manufacturer.
   2. Satisfaction of the above requirements shall not relieve the Contractor of responsibility for incorrect installation, defective equipment items, or collateral damage as a result of Contractor work efforts.

B. Supplemental Contractor Quality Control: The following requirements supplement the Contractor quality control requirements specified elsewhere in the contract:
   1. The Contractor shall provide the services of technical representatives who are familiar with all components and installation procedures of any installed Security Access Detection; and are approved by the Contracting Officer.
   2. The Contractor will be present on the job site during the preparatory and initial phases of quality control to provide technical assistance.
   3. The Contractor shall also be available on an as needed basis to provide assistance with follow-up phases of quality control.
   4. The Contractor shall participate in the testing and validation of the system and shall provide certification that the system installed is fully operational as all construction document requirements have been fulfilled.

C. All testing and training shall be compliant with the VA General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.

D. The Commissioning Agent will observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the Resident Engineer and Commissioning Agent. Provide a minimum of 7 days prior notice.

3.9 COMMISSIONING

A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up, and contractor testing required above and required by the System Readiness Checklist provided by the Commissioning Agent.

B. Components provided under this section of the specification will be tested as part of a larger system. Refer to Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for contractor responsibilities for system commissioning.

-----END----

28 16 00 INTRUSION DETECTION FOR ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0, City of Austin, Texas

January, 2014

1 PART 1 - GENERAL

1.1 DESCRIPTION

A. Provide and install a complete Intrusion Detection System, hereinafter referred to as IDS, as specified in this section.

B. This Section includes the following:

   1. Intrusion detection with modular, microprocessor-based controls, intrusion sensors and detection devices, and communication links to perform monitoring, alarm, and control functions.

   2. Responsibility for integrating electronic and electrical systems and equipment is specified in the following Sections, with Work specified in this Section:

      a. Division 08 Section "DOOR HARDWARE".

      b. Division 14 Section "ELECTRIC TRACTION ELEVATORS".

      c. Division 27 Section "INTERCOMMUNICATIONS AND PROGRAM SYSTEMS".

      d. Division 28 Section "PHYSICAL ACCESS CONTROL".

      e. Division 28 Section "FIRE DETECTION AND ALARM".

      f. Division 28 Section "VIDEO SURVEILLANCE".

      g. Division 32 Section "CHAIN LINK FENCES AND GATES".

C. Related Sections include the following:

   1. Division 28 Section "VIDEO SURVEILLANCE" for closed-circuit television cameras that are used as devices for video motion detection.

   2. Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY" for cabling between central-station control units and field-mounted devices and controllers.

1.2 RELATED WORK

SPECS WRITER NOTE: Delete any item or paragraph not applicable in the section.

A. Section 01 00 00 - GENERAL REQUIREMENTS. For General Requirements.

B. Section 07 84 00 - FIRESTOPPING. Requirements for firestopping application and use.

C. Section 14 21 00 - ELECTRIC TRACTION ELEVATORS. Requirements for elevators.

D. Section 14 24 00 - HYDRAULIC ELEVATORS. Requirements for elevators.

E. Section 10 14 00 - SIGNAGE. Requirements for labeling and signs.

F. Section 26 05 11 - REQUIREMENTS FOR ELECTRICAL INSTALLATIONS. Requirements for connection of high voltage.

G. Section 26 05 21 - LOW VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES (600 VOLTS AND BELOW). Requirements for power cables.

H. Section 28 05 00 – COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY. Requirements for general requirements that are common to more than one section in Division 28.

I. Section 28 05 13 - CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for conductors and cables.

J. Section 28 05 26 - GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY. Requirements for grounding of equipment.

K. Section 28 05 28.33 - CONDUITS AND BACKBOXES FOR ELECTRONIC SAFETY AND SECURITY. Requirements for infrastructure.

L. Section 28 08 00 - COMMISIONING OF ELECTRONIC SAFETY AND SECURITY. Requirements for commissioning - systems readiness checklists, and training.

M. Section 28 13 00 - PHYSICAL ACCESS CONTROL SYSTEMS (PACS). Requirements for physical access control integration.

N. Section 28 13 16 - ACCESS CONTROL SYSTEM AND DATABASE MANAGEMENT. Requirements for control and operation of all security systems.

O. Section 28 23 00 - VIDEO SURVEILLANCE. Requirements for security camera systems.

P. Section 28 26 00 - ELECTRONIC PERSONAL PROTECTION SYSTEM (EPPS). Requirements for emergency and interior communications.

Q. Section 28 31 00 - FIRE DETECTION AND ALARM. Requirements for integration with fire detection and alarm system.

1.3 QUALITY ASSURANCE

A. See Division 28 05 00 COMMON WORK RESULTS

1.4 DEFINITIONS

A. Controller: An intelligent peripheral control unit that uses a computer for controlling its operation. Where this term is presented with an initial capital letter, this definition applies.

B. I/O: Input/Output.

C. Intrusion Zone: A space or area for which an intrusion must be detected and uniquely identified, the sensor or group of sensors assigned to perform the detection, and any interface equipment between sensors and communication link to central-station control unit.

D. LED: Light-emitting diode.

E. NEC: National Electric Code

F. NEMA: National Electrical Manufacturers Association

G. NFPA: National Fire Protection Association

H. NRTL: Nationally Recognized Testing Laboratory.

I. SMS: Security Management System – A SMS is software that incorporates multiple security subsystems (e.g., physical access control, intrusion detection, closed circuit television, intercom) into a single platform and graphical user interface.

J. PIR: Passive infrared.

K. RF: Radio frequency.

L. Standard Intruder: A person who weighs 45 kg (100 lb.) or less and whose height is 1525 mm (60 in) or less; dressed in a long-sleeved shirt, slacks, and shoes.

M. Standard-Intruder Movement: Any movement, such as walking, running, crawling, rolling, or jumping, of a "standard intruder" in a protected zone.

N. TCP/IP: Transport control protocol/Internet protocol incorporated into Microsoft Windows.

O. UPS: Uninterruptible Power Supply

P. UTP: Unshielded Twisted Pair

1.5 SUBMITTALS

SPEC WRITER NOTE: Delete and/or amend all paragraphs and sub-paragraphs and information as needed to ensure that only the documentation required is requested per the Request for Proposal (RFP).

A. Refer to Section 28 05 00, Part1

1.6 APPLICABLE PUBLICATIONS

The publications listed below (including amendments, addenda, revisions, supplement, and errata) form a part of this specification to the extent referenced. The publications are referenced in the text by the basic designation only.

A. American National Standards Institute (ANSI)/Security Industry Association (SIA):

PIR-01-00	Passive Infrared Motion Detector Standard - Features for Enhancing False Alarm Immunity
CP-01-00	Control Panel Standard-Features for False Alarm Reduction

B. Department of Justice American Disability Act (ADA)

28 CFR Part 36	2010 ADA Standards for Accessible Design

C. Federal Communications Commission (FCC):

(47 CFR 15) Part 15 Limitations on the Use of Wireless Equipment/Systems

D. National Electrical Manufactures Association (NEMA):

250-08 Enclosures for Electrical Equipment (1000 Volts Maximum)

E. National Fire Protection Association (NFPA):

70-11 National Electrical Code

731-08 Standards for the Installation of Electric Premises Security Systems

F. Underwriters Laboratories, Inc. (UL):

464-09 Audible Signal Appliances

609-96 Local Burglar Alarm Units and Systems

634-07 Standards for Connectors with Burglar-Alarm Systems

639-07 Standards for Intrusion Detection Units

1037-09 Standard for Anti-theft Alarms and Devices

1635-10 Digital Alarm Communicator System Units

G. Uniform Federal Accessibility Standards (UFAS), 19841.

1.7 COORDINATION

A. See Division 28 05 00, Section 1.8 COORDINATION

1.8 EQUIPMENT AND MATERIALS

A. See Division 28 05 00, Section 1.13 EQUIPMENT AND MATERIALS

1.9 WARRANTY OF CONSTRUCTION

A. See Division 28 05 00, Section 1.20 WARRANTY

2 PART 2 – PRODUCTS

SPEC WRITER NOTE: Delete or amend all paragraphs and sub-paragraphs as needed to ensure that only the equipment required per the Request for Proposal (RFP) is provided.

2.1 FUNCTIONAL DESCRIPTION OF SYSTEM

SPEC WRITER NOTE: Revise functional description to fit the project requirements.

A. Supervision: System components shall be continuously monitored for normal, alarm, supervisory, and trouble conditions. Indicate deviations from normal conditions at any location in system. Indication includes identification of device or circuit in which deviation has occurred and whether deviation is an alarm or malfunction.

SPEC WRITER NOTE: Retain subparagraphs below if retaining option in paragraph above.

    1. Alarm Signal: Display at central-station control unit and actuate audible and visual alarm devices.
    2. Trouble Condition Signal: Distinct from other signals, indicating that system is not fully functional. Trouble signal shall indicate system problems such as battery failure, open or shorted transmission line conductors, or controller failure.
    3. Supervisory Condition Signal: Distinct from other signals, indicating an abnormal condition as specified for the particular device or controller.

SPEC WRITER NOTE: Select one of the first two paragraphs below.

B. System Control: Central-station control unit shall directly monitor intrusion detection units and connecting wiring.

C. System shall automatically reboot program without error or loss of status or alarm data after any system disturbance.

D. Operator Commands:

SPEC WRITER NOTE: Edit list below to suit Project. Coordinate with operator commands listed for "Central-Station Control Units" Article. Delete nonapplicable commands.

    1. Help with System Operation: Display all commands available to operator. Help command, followed by a specific command, shall produce a short explanation of the purpose, use, and system reaction to that command.
    2. Acknowledge Alarm: To indicate that alarm message has been observed by operator.
    3. Place Protected Zone in Access: Disable all intrusion-alarm circuits of a specific protected zone. Tamper circuits may not be disabled by operator.
    4. Place Protected Zone in Secure: Activate all intrusion-alarm circuits of a protected zone.
    5. Protected Zone Test: Initiate operational test of a specific protected zone.
    6. System Test: Initiate system-wide operational test.
    7. Print Reports.

SPEC WRITER NOTE: Coordinate function in paragraph below with timing device specified in "Central-Station Control Units" Article.

E. Timed Control at Central-Station Control Unit: Allow automatically timed "secure" and "access" functions of selected protected zones.

SPEC WRITER NOTE: Retain paragraph and subparagraphs below if alarm signals control lights, elevators, intercom, sound, or closed-circuit television components. Edit to suit Project design and systems integration specifications. Coordinate with Drawings.

F. Automatic Control of Related Systems: Alarm or supervisory signals from certain intrusion detection devices control the following functions in related systems:

    1. Switch selected lights.
    2. Open a signal path between certain intercommunication stations.
    3. Switch signal to selected monitor from closed-circuit television camera in vicinity of sensor signaling an alarm.

SPEC WRITER NOTE: Delete paragraph below if no printer in system.

G. Response Time: 2 seconds between actuation of any alarm and its indication at central-station control unit.

H. Circuit Supervision: Supervise all signal and data transmission lines, links with other systems, and sensors from central-station control unit. Indicate circuit and detection device faults with both protected zone and trouble signals, sound a distinctive audible tone, and display a visual signal. Maximum permissible elapsed time between occurrence of a trouble condition and indication at central-station control unit is 20 seconds. Initiate an alarm in response to opening, closing, shorting, or grounding of a signal or data transmission line.

SPEC WRITER NOTE: Delete paragraph below if not required for the Project. Coordinate with Drawings.

I. Programmed Secure-Access Control: System shall be programmable to automatically change status of various combinations of protected zones between secure and access conditions at scheduled times. Status changes may be preset for repetitive, daily, and weekly; specially scheduled operations may be preset up to a year in advance. Manual secure-access control stations shall override programmed settings.

J. Manual Secure-Access Control: Coded entries at manual stations shall change status of associated protected zone between secure and access conditions.

2.2 SYSTEM COMPONENT REQUIREMENTS

SPEC WRITER NOTE: Retain first paragraph and subparagraph below if systems integration is required. If retaining, identify equipment and Section that specifies integrated system console.

A. Compatibility: Detection devices and their communication features, connecting wiring, and central-station control unit shall be selected and configured with accessories for full compatibility with the following equipment:

    1. Data Gathering Panel, Output Module, Input Module, 28 13 00 PHYSICAL ACCESS CONTROL SYSTEM.

    2. //List devices…//

B. Surge Protection: Protect components from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include surge protection for external wiring of each conductor entry connection to components.

    1. Minimum Protection for Power Lines 120 V and More: Auxiliary panel suppressors complying with requirements in Division 26 Section TRANSIENT-VOLTAGE SUPPRESSION FOR LOW-VOLTAGE ELECTRICAL POWER CIRCUITS.

    2. Minimum Protection for Communication, Signal, Control, and Low-Voltage Power Lines: Comply with requirements in Division 26 Section TRANSIENT-VOLTAGE SUPPRESSION FOR LOW-VOLTAGE ELECTRICAL POWER CIRCUITS as recommended by manufacturer for type of line being protected.

C. Interference Protection: Components shall be unaffected by radiated RFI and electrical induction of 15 V/m over a frequency range of 10 to 10,000 MHz and conducted interference signals up to 0.25-V RMS injected into power supply lines at 10 to 10,000 MHz.

SPEC WRITER NOTE: Coordinate paragraph below with Drawings and detailed component Specifications.

D. Tamper Protection: Tamper switches on detection devices, controllers, annunciators, pull boxes, junction boxes, cabinets, and other system components shall initiate a tamper-alarm signal when unit is opened or partially disassembled and when entering conductors are cut or disconnected. Central-station control-unit alarm display shall identify tamper alarms and indicate locations.

SPEC WRITER NOTES: Coordinate three paragraphs below with Drawings and with features listed in central-station control units and at central-station control unit. Delete items not in Project. Indicate features in a device schedule.

E. Self-Testing Devices: Automatically test themselves periodically, but not less than once per hour, to verify normal device functioning and alarm initiation capability. Devices transmit test failure to central-station control unit.

F. Addressable Devices: Transmitter and receivers shall communicate unique device identification and status reports to central-station control unit.

SPEC WRITER NOTE: Delete paragraph below unless remotely adjustable detectors are used.

2.3 ENCLOSURES

A. Interior Sensors: Enclosures that protect against dust, falling dirt, and dripping noncorrosive liquids.

B. Interior Electronics: NEMA 250, Type 12.

C. Exterior Electronics: NEMA 250, Type 4X [fiberglass] [stainless steel].

D. Corrosion Resistant: NEMA 250, Type 4X [PVC] [stainless steel].

E. Screw Covers: Where enclosures are accessible to inmates, secure with security fasteners of type appropriate for enclosure.

2.5 EQUIPMENT ITEMS

A. General:

1. All requirements listed below are the minimum specifications that need to be met in order to comply with the IDS.
2. All IDS sensors shall conform to UL 639, Intrusion Detection Standard.
3. Ensure that IDS is fully integrated with other security subsystems as required to include, but not limited to, the CCTV, PACS, EPPS, and Physical Access Control System and Database Management. The IDS provided shall not limit the expansion and growth capability to a single manufacturer and shall allow modular expansion with minimal equipment modifications.

B. IDS Components: The IDS shall consist of, but not be limited to, the following components:

1. Control Panel
2. Exterior Detection Devices (Sensors)
3. Interior Detection Devices (Sensors)
4. Power Supply
5. Enclosures

2.4 CONTROL PANEL

A. The Control panel shall be the main point of programming, monitoring, accessing, securing, and troubleshooting the IDS. Refer to American National Standards Institute (ANSI) CP-01 Control Panel Standard-Features for False Alarm Reduction.

B. The Control Panel shall provide a means of reporting alarms to a Physical Access Control System and Database Management system via a computer interface or direct connection to an alarm control monitoring panel.

C. The Control panel shall utilize a Multifunctional Keypad, Input and Output Modules for expansion of alarm zones, interfacing with additional security subsystems, programming, monitoring and controlling the IDS.

D. The Control panel shall meet or exceed the following minimum functional requirements for programming outputs, system response, and user interface:

1. Programming Outputs:
    a. (2) Amps alarm power at 12 VDC
    b. (1.4) Amps auxiliary power at 12 VDC
    c. (4) alarm output patterns
    d. Programmable bell test
    e. Programmable bell shut-off timer
2. System Response:
    a. Selectable point response time
    b. Cross point capability
    c. Alarm verification
    d. Watch mode
    e. Scheduled events arm, disarm, bypass and un-bypass points, control relays, and control authority levels
3. User Interface:
    a. Supervises up to eight command points (e.g. Up to 16 unsupervised keypads can be used)
    b. Provides custom keypad text
    c. Addresses full function command menu including custom functions
    d. Allows user authority by defined area and 16-character name
    e. Provides for 14 custom authority control levels allowing user's authority to change, add, delete pass codes, disarm, bypass points, and start system tests.
4. The Control panel shall meet or exceed the following technical characteristics:

Input Voltage via 110 VAC or 220 VAC Step-down Transformer	16 or 18 VAC
Operating Voltage	12 VDC
Output Voltage	12 VDC @ 2 A max

Direct Hardwire Zones	7
Partitions	8
Multifunctional Keypads	16 (2 per partition)
Communications Port	RJ-11

E. A multifunctional keypad shall be utilized as a user interface for arming, disarming, monitoring, troubleshooting, and programming the alarm control panel.

F. Keypads shall have the following features:

1. Multiple function keypads suitable for remote mounting, no greater than 1333 m (4000 ft), shall be provided from the control panel and have a light emitting diode (LED) readout of alarm and trouble conditions by zone.
2. An alphanumeric English language display, with keypad programmability, and EE-PROM memory, shall also be provided.
3. Trouble alarm indicators shall be distinguishable from intrusion alarms.
4. A minimum of four (4) zones selectable as entry and exit with programmable time delay.
5. Complete system test activated capability at the keypad.
6. Capability for opening and closing reports to a remote monitoring location.
7. Adjustable entry and exit delay times.
8. Capability for a minimum of two (2) multiple function keypads.
9. Capability to shunt or bypass selected interior zones while arming perimeter protection and remaining interior zones.
10. Capability for a minimum of seven assignable pass-codes that are keypad programmable from a suppressed master code.
11. The control panel shall have a communications port that will allow for communications with a computer for programming, monitoring, and troubleshooting purposes. The communications port will be, at a minimum, and RJ-11 or better.
12. The control panel will have a systems success probability of 95% or better, and shall include the following success considerations:
    a. False Alarm: Shall not exceed one (1) false alarm per 30 days per sensor zone.
    b. Nuisance Alarm: Shall not exceed a rate of one (1) alarm per seven (7) days per zone within the first 60 days after installation and acceptance. Sensor adjustments will be made and then shall not exceed one (1) alarm per 30 days.
13. The Control Panel will be able to detect either a line fault or power loss for all supervised data cables.
    1. Line Fault Detection: Communication links of the IDS shall have an active mode for line fault detection. Fault isolation at the systems level shall have the same geographic resolutions as provided for intrusion detection. The line fault alarm shall be clearly distinguishable from other alarms.

2. Power Loss Detection: Provide the capability to detect when critical components experience temporary or permanent loss of power and annunciate to clearly identify the component experiencing power loss.

2.5 KEYPADS

A. Keypads shall meet or exceed the following technical characteristics:

Connections	4-wire flying lead for data and power
Operating Temperature	0°C to +50°C (+32°F to +122°F)
Display Window	8-point LED
Indicators: Illuminated keys	Armed Status-LED
	Point Status-LED
	Command Mode-LED
	Power-LED
Voltage	Nominal 12 VDC

2.6 INPUT MODULE

A. An input module shall be utilized to connect additional detection devices to the control panel. This module will meet or exceed the following technical characteristics:

B. Operating Voltage	C. 8.5 to 14.5 VDC Nominal
D. Zone Inputs	E. Style A (Class B) Supervised
F. Operating Temperature	G. 0 to 40 degrees C (32 to 140 degrees F)

2.7 OUTPUT MODULE

A. An output module shall be utilized to interface the control panel with other security subsystems. The output module shall meet or exceed the following technical characteristics:

Operating Voltage	8.5 to 14.5 VDC Nominal
Output Relays	“Form C” Dry Relay Contracts
Relay Contact Rating	4A @ 24 VDC
	4A @ 24 VAC
	1A @ 70 VAC
Operating Temperature	0 to 40 degrees C F (32 to 140 degrees)

2.8 EXTERIOR DETECTION DEVICES (SENSORS)

A. The IDS shall consist of interior, exterior, and other detection devices that are capable of:

  1. Locating intrusions at individually protected asset areas or at an individual portal;
  2. Locating intrusions within a specific area of coverage;
  3. Locating failures or tampering of individual sensors or components.

B. Audible annunciation shall meet UL 464 Audible Signal Appliance requirements as well as other stated within this specification. IDS shall provide and adjust for devices so that coverage is maximized in the space or area it is installed in. For large areas where multiple devices are required, ensure exterior device coverage is overlapping.

C. Detection sensitivity shall be set up to ensure maximum coverage of the secure area is obtained while at the same time limiting excessive false alarms due to the environment and impact of small animals. All detection devices shall be anti-masking with exception of video motion detection.

D. Dual sensor technology shall be used when possible. Sensor technology shall not be of the same type that is easily defeated by a single method. This will reduce the amount of false alarms.

E. Exterior sensors described in this section are intended for outdoor use for perimeter and fence control monitoring purposes. Some sensors described in the interior sensor section may be utilized that can provide both outdoor and indoor protection.

F. External Sensors Environmental Characteristics:

Temperature	-25°F - 140°F (-32°C - 60°C)
Pressure	Sea Level to 15,000 ft. (4573m) above sea level
Solar Radiation	Six (6) hrs. exposure at dry bulb temp. 120°F (60°C)
Rain	Two (2) in. (50 mm) per hour
Humidity	5% - 95%
Fungus	Components of non-fungus nutrient materials
Salt/fog	Atmosphere 5% salinity
Snow loading	48 lbs per sq. ft. (234 kg per sq. meter)
Ice accumulation	Up to ½ in. (12.7 mm) radial ice
Wind limitations	50 mph (80 km/h) Gusts to 66 mph (106 km/h)
Acoustical Noise Suitability	> 110 decibels (dB)

G. Electromechanical Fence Sensors

  1. Electromechanical Fence Sensors: Shall sense mechanical vibrations or motion associated with scaling, cutting, or attempting to lift standard security chain link fence as follows: Note: Dead zones shall not exist from a monitoring and alarm coverage perspective.

2. The sensor zone control unit shall alarm when a sufficient number of sensing unit activations surface within a specified time period.
3. Individual sensing units and the alarm thresholds shall be field adjustable (i.e., performed by an authorized technician or trained maintenance personnel). Midrange sensitivity settings shall alarm a sensor when an intruder attempts to scale or climb the fence in areas of reduced sensitivity (e.g. around poles and rigid supports, etc.) and attempted lifting or scaling of a fence, including using assisted methods (e.g. items leaned against the fence, etc.)occur. Sensors shall allow gradual changes in fence positioning due to expansion, settling, and aging, without increased numbers of nuisance alarms taking place.
4. Exterior sensor components shall be housed in rugged, corrosion-resistant enclosures, protected from environmental impact and degradation.
5. Fence cable support hardware shall be weather-resistant. Interfacing between sensor zones and alarm enunciators, require they be installed in underground conduit and cables.
6. Fencing Cable Technical Characteristics:

Input voltage	12-30 V DC
Current requirement	4 mA quiescent 25 mA (max) in alarm
Transient suppression	On data, power input lines and on relay output
Enclosure	Weatherproof
Sensor type	Inertial band-pass-filter
Transponder	4 zone controller Output relays for dry contacts, or RS-485 communication Inputs for weather sensor
Sensor spacing	2.5 to 3 m (8.2 to 9.9 ft.)
Data I/O	RS 485 communications
Data output	• Vibration alarm (in either line) • Line alarm (in either line) • End of line action • Wind situation • Weather sensor line failure • Enclosure tamper switch • Program fail • A dry contact output with end of line resistor per each of

	4 vibration inputs

H. Strain Sensitive Cable Sensors

1. Strain-Sensitive Cable Sensors: These devices shall detect movement on a standard security chain link fence associated with an intruder scaling, cutting through, or attempting to lift the fence fabric. The entire sensor system shall be mounted directly on the fence and able to withstand the same environmental condition exposures. Note: The length of the fence shall also maintain no sensor monitoring dead zones.

    a. Individual sensing units and the alarm threshold shall be field adjustable (i.e. by authorized technicians or trained maintenance personnel) for compensation of winds up to 40km/h (25 mph) or by zone without increased nuisance alarms while maintaining specified sensor performance as under ambient conditions.

    b. Sensor zone control units shall provide an analog audio output for interface to an external audio amplifier to permit remote audio assessment regardless of sensor alarm status. The sensor zone control unit alarm output interface shall be a separately supervised relay contact normally open or normally closed.

    c. The length of the fence shall be divided into 100m (300 ft) zones.

    d. The sensing unit shall consist of transducer cable capable of achieving specified performance either by attachment directly to the fence fabric by plastic cable every 300 to 455 mm (12 to 18 inches) or by installation inside electrical metallic tubing conduit mounted on the fence.

    e. The sensing unit shall have equal adjustable sensitivity throughout the entire fence length. Only conventional waterproof coaxial cable connectors shall be used for connections of the sensing unit to avoid electrical magnetic interference.

    f. The entire sensor system shall be tamper resistant and capable of detecting tampering within each portion of the system by sensor zone.

    g. Magnetic Sensor Cable Technical Characteristics:

Magnetic Sensor Cable	
Type cable	Four (4) conductor magnetically loaded, aluminum foil shield and ground wire
Maximum zone length	300 m (1000 ft.)
Life expectancy	10 years
Sensitivity	Uniform over length of cable
Audio Bandwidth	Five (5) kHz
Outer Cover	Black Polyurethane, Ultraviolet resistant
Insensitive Cable (remote processing)	
Type cable	2 twisted pair, individually sealed
Outer Cover	Black Polyurethane, Ultraviolet resistant

Dual Channel Signal Processor	
Input Power	10.2 – 13.8 VDC 65 mA
Alarm Output	Alarm contacts SPNC 0.75 mA, 200 VDC
Indicators	Three (3):Alarm, tamper, events
Cut processor	Sensitivity - 10 settings Time window – 0.5 – 4.5 min Event Counter – nine (9)
Climb processor	Sensitivity – 10 settings

I. Buried Electromagnetic Cable Sensor

1. The system shall be able to function as a standalone system or as an integral component of a centralized security control system.
2. The detection field shall be formed by radio-frequency (RF) signals carried by sensor cables that are buried along the perimeter.
3. The RF signals shall form an invisible electromagnetic detection field around the sensor cables that can detect the presence of an intruder passing through the field.
4. The system shall detect moving intruders that have a significant electromagnetic field (e.g. humans, vehicles, and other large conductive objects) while rejecting other environmental stimuli such as birds, small animals, weather elements.
5. A sensor module shall contain the electronics required to:
   a. Transmit and receive the RF signal without the use of an external antenna.
   b. Monitor the detection fields of two (2) zones and produce an alarm when an intruder enters the zones.
6. Field power modules shall be available for standalone systems and networked systems.
7. As a standalone system, the primary operator interface shall be a local interface module that is connected directly to the sensor module.
8. As part of a network configuration, the primary operator interface shall be a personal computer (PC) based central controller. The central controller shall monitor the performance of the entire buried coaxial cable outdoor intrusion detection system and any auxiliary sensors. The central controller shall have the capability of acknowledging, processing and reporting alarms. A customized color site map that is displayed on the PC monitor shall be an available option for the system to monitor sensor locations.
9. Transmission and reception shall be accomplished without the use of antennae. The RF signal shall be monitored and analyzed by the sensor module for any changes in the detection field properties that would indicate the presence of an intruder.
10. Alarms generated by internal electronic processes (cables excluded) shall not exceed one (1) per zone per month. System generated alarms are averaged based on the total number of zones in the system.

11. When the system is calibrated in accordance with the manufacturers' recommendations, the detection field shall be continuous and uniform over the protected site perimeter.

12. When system sensitivity is calibrated according to manufacturers' recommendations, the detection field shall not detect a valid target that is a minimum of 2 m. (6.5 ft) from the nearest sensor cable.

13. Buried Electromagnetic Cable Sensor Technical Characteristics:

Burial Medium	Clay, sand, soil, asphalt, concrete
Snow limitation	Up to 30c. (1 foot) deep
Degradation Guaranty	Minimum 10 yr.
Detection Medium	Radio Frequency (RF)
Detection Coverage	Maximum 200m (656 ft.) per zone
Detection Capability	Human: >34 kg. (75 lbs)
Detection Speed	Human walk, crawl, run, roll, jump 2.5 cm/sec (1 in./sec.) –15 m/sec (50 ft./sec.) regardless of direction across field
Velocity Response	Programmable
Detection Probability	Human: 99% with 95% confidence factor Animal: Less than 10 kg. (22 lbs.) Less than 5% with 90% confidence factor
Terrain Detection Capabilities	Even to uneven ground with maximum (max) grade 4 m (13 ft.) Corner bend radius 6.5m (22 ft.)
Detection Field Cross Section	Upright walking; Height1m: (3.2 ft.) above ground Width: 2m (6.5 ft.) single cable 3m. (9.75 ft) double cable
Sensing Element	Ported (leaky) coaxial cables
Cable Construction	Abrasion and chemical resistant, high density polyethylene, with flooding compound
Cable Requirements	Two (2):Transmit cable, receive cable
Configurations Available	Two (2):Single cable, double cable
Cable Lengths	50 m (164 ft.), 100 m (328 ft.), 150 m (492 ft.), 200 m (656 ft.)
Zone Length Minimum	10 m (33 ft.)

Antenna Requirements	None
False alarm rate	Less than one (1) per day

14. Sensor Module: Each sensor module shall transmit, receive and process the electromagnetic detection fields independently from other sensor modules. Failure of one (1) sensor module shall not affect the remainder of the perimeter. The sensor module shall operate as either a standalone unit, or in a network configuration in conjunction with a central controller. The sensor module shall be mounted in a weatherproof enclosure when installed outdoors as follows.
15. The sensor module shall use an adaptive filter to analyze the detection signal and adjust the signal processing to reduce nuisance alarms caused by environmental factors such as rainfall or slow-running water.
16. The sensor module shall identify, by type, sensor, tamper, and failure alarms either locally at the sensor module, or centrally at a central controller. The sensor cables shall provide the data paths between the sensor modules, for the transmission, reception and display of alarm conditions.
17. Each sensor module shall include an internal interface for the collection of auxiliary sensor data.
18. It shall be possible to supply power directly to each unit for applications that require either a single sensor module or multiple sensor modules with independent power sources.
19. The sensor module's response shall be demonstrated by an analog output signal that can be displayed on a voltmeter or on an analog voltage-recording device. The output signal shall be encoded to indicate the alarm trip-point, thereby showing the sensor module's degree of detection above or below the level required to cause an alarm.
20. Sensor Module Technical Characteristics:

Sensor Module Power Output	12 VDC at 150 milliampere (mA)
Sensor Module Power Requirements	Stand-alone: 12 VDC 500 mA max Network: 48 VDC 175 mA max
Sensor capability	Two (2) zones independent of other sensor modules
Sensor coverage	400 m. (1,312 ft)
Calibration	Locally and remotely from Central Controller
Self Test	Via 4 relay drive points
Detection coverage	Unlimited expansion using multiple modules
Nuisance avoidance	Adaptive filtering
Connectivity	RS-485 twisted pair cable
Sensor Support	Dual redundant data paths
Transmission capability	Eight (8) contact-closure signals

21. The field power module shall be capable of supplying power to sensor modules as follows:

a. In a network configuration where power is supplied redundantly via the sensor cables, the sensor modules shall operate within specifications when power is removed from either of the two (2) sensor cables.

b. Each cable zone shall be capable of being calibrated either locally at the sensor module, or remotely from a central controller. Additional signal processing parameters, including high speed and low speed response, shall be capable of being set from a central controller.

c. Detection sensitivity for each zone shall be adjusted either locally at the sensor module with a local interface module, or from a central controller. Access to the local calibration controls shall require the removal of the enclosure's cover and shall cause a tamper alarm to be generated.

d. Power Module Technical Characteristics:

Output support	Nine (9) sensor modules max 2,800 m (3,063 yards)
System block configuration	1,400 m (1,531 yds.)
Power Output	Stand-alone: 12 VDC 500 mA max Network: 48 VDC 175 mA max

J. Microwave Sensors

1. The system shall be a modular microwave outdoor intrusion detection sensor based on microwave radar technology. The detection field shall be formed by radio frequency (RF) signals, in the X-band, carried between a transmitter and a receiver. The RF signals shall form an invisible electromagnetic detection field that can detect the presence of an intruder who walks, crawls, rolls, jumps, or runs through a detection field as follows.

   a. Transmitter shall create the RF signals that form the detection field. A receiver shall house the necessary electronics to monitor the detection field and to raise an alarm when an intruder enters the field. The transmitter and receiver shall be powered individually, as a standalone unit.

   b. An electromagnetic wave is emitted by the antenna of the transmitter and received by the antenna of the receiver. The receiver shall detect changes that are caused by the presence of an intruder.

   c. The system shall detect moving intruders having a significant electromagnetic cross-section (e.g. humans, vehicles, and other large conductive objects) rejecting other environmental stimuli.

   d. The system shall be capable of detecting human intruders moving through the detection field regardless of the direction of motion.

   e. Processor description: The receiver shall contain the necessary electronics to perform the signal processing for the detection zone. The transmitter and receiver shall be operated as a standalone unit with independent power and data. Both the transmitter and receiver shall be installed in weatherproof enclosures.

f. Distributed processing: Transmitter-receiver pairs distributed along a perimeter shall provide extended range and fail-safe operation. The failure of one (1) pair shall not affect the coverage of the remainder of the perimeter.

g. Alarms: The signal processor shall identify intrusion and tamper/fail alarms locally, at the transmitter or receiver.

   1) An alarm caused by opening the outer enclosure of the transmitter or receiver shall be identified as a tamper alarm. Tamper alarms shall be distinctive from intrusion alarms.

   2) Alarms caused by power failure or internal electronic failure are fail alarms, distinctive from intrusion alarms.

h. Microwave Sensor System Technical Characteristics:

Operating voltage Transmitter	11 – 15 VDC 70mA max. current
Operating voltage Receiver	11 – 15 VDC 30mA max. current
Operating Environment	–30ºC (-22F) and 60ºC (140 F)
LEDs	POWER ON, WRONG CHANNEL, ALARM
Maximum zone length	10 m (33 ft.) and a maximum of 457 m (1500 ft.) per zone.
Detection Success Probability	34 kg (75 lbs.) 99% with a 95% confidence factor
Operating frequency	X Band 10.525 ± 0.025 gigahertz (GHz)
Type modulation	Class A2 with one (1) of six (6) selectable crystal-controlled frequencies.
Detection movement speed	5 cm/sec. (2.0 in. sec.) to 8 m/sec. (26 ft. sec.)
Audio assessment	Via 1/8 in. phone jack on receiver
Alarms	Tamper, failure, intrusion
Tamper/fail alarm	Via sealed relay rated one (1) ampere 28 VDC
Intrusion field alarm	Via sealed relay rated two (2) ampere 28 VDC.
Intrusion alarm latch time	Adjustable: 0.5 sec and 10 sec
Processing	Distributed: receiver/transmitter pairs
Perimeter Length	Single Receiver/transmitter pair: 457 m (1500 ft.) Multiple pairs: Unlimited

K. Taut-Wire Sensors

1. These sensors shall consist of a perimeter intrusion detection sensor incorporated into a wire security fence. Intrusion detection shall be achieved by sensing the cutting of any single wire or deflection of the fence, such as by climbing.

a. Sensor zone: Includes one (1) or more 61 m (200 ft.) maximum sections of 2.3 m (seven (7) ft.) high parallel fence. Each sector shall consist of 13 horizontal barbed wires attached to the taut-wire fence posts, and three (3) strands as outriggers, and an "anti-ladder" trip wire supported by rods extending from the outriggers for a total vertical height of approximately 2.6 m (eight (8) ft.).

b. Displacement switches for each horizontal wire shall be mounted 2within a pre-wired channel fastened to the fabric fence post at the midpoint of each section. Outrigger barbed wire and tripwire may share the same switch in these locations.

c. Abnormal displacement of a switch lever resulting from cutting or deflecting its attached wire, as by climbing on or through fence strands, shall initiate an alarm condition. A damping mechanism within the sensor shall reduce alarm thresholds due to slowly changing environmental phenomena such as the ground shifting, daily and seasonal temperature variations, winds changes, etc.

d. Sensor switches shall be provided with electrical contact closures as a means for initiating an alarm condition.

e. The system shall provide relay outputs to interface alarm outputs with the overall IDS.

f. Taut-wire Sensor Technical Characteristics:

Power requirements	Input: 120 – 208 VAC
Sensor zone control unit capability	Up to 10 zones
Sensitivity	19 mm (0.75 in.)
Environment Limits	Winds up to 56 km/h (35 mph)

L. Electrostatic Field Sensors

1. These sensors generate an electrostatic field around one (1) or more horizontal wires and detect intrusion of the electrostatic field as follows.

a. Sensors shall initiate an alarm when an intruder attempts to approach or scale a fence or physical barrier. Electrostatic field sensors shall detect human presence by generating an electric field around one (1) or more horizontal wires that detects the induced signal in parallel sensing wires.

b. Sensors shall monitor the induced signal for changes that result from the presence of a human body, which distorts coupling between transmitting and sensor wires.

c. Sensor components shall consist of one (1) or more signal generator field wires and mounting hardware, sensing wires, an amplifier/signal processors, power supplies, and necessary circuitry hardware. Mounting and support hardware shall be provided by the equipment manufacturer.

d. Wires shall be spring tension-mounted and provided with end-of-line terminators to detect cutting, shorting, or breaking of the wires.

e. Sensor configuration shall be able to detect an intruder that may crawl under the bottom wire, through the wires, or over the top wire by divided sensor zones.

f. Signal processing circuitry shall provide filtering to distinguish nuisance alarms.

g. Sensor configuration shall incorporate balanced, opposed field construction to eliminate distant field noise.

h. Sensor sensitivity shall be adjustable. Adjustment controls shall be inaccessible to operating personnel and system sensitivity controls shall be set at approximately midrange.

i. Sensors shall provide some means of indicating an alarm condition at the protected perimeter to facilitate installation and calibration.

j. The sensor system shall include an indicator disabling device within a tamperproof enclosure.

k. Electrostatic Field Sensor Technical Characteristics:

Power	115 -120 VAC transformer
Operating Power Requirements	16-22 VAC, 225 mA single zone 275 dual zone
Detection Sensitivity	77 lbs within 915 mm (3 ft.)- midrange setting
Detection Velocity	30 m (0.1 ft.) - 300 m (10 ft.) per sec
Supervision	AC Monitoring of fence and field wires – open, short, and grounded circuits
Tamper Switch	One (1)-pole, two (2) position
Lightening arrestor	Transistors on all relay output and power inputs
Battery Charger	Built-in
Processor Enclosure	Base plate, steel NEMA enclosure Weather resistant

M. Gate Sensors

1. They shall be provided in accordance with specific fence sensor manufacturer's recommendations to ensure continuous fence sensor zone protection for the entire protected perimeter.

   a. When gate units are not provided by the fence sensor manufacturer, provide separately zoned Balanced Magnetic Switch (BMS) gate sensors.

   b. Sensors shall perform as specified in Section 2.3-E.6 entitled "Balanced Magnetic Switches (BMS)."

2.9 INTERIOR DETECTION DEVICES (SENSORS)

A. The IDS shall consist of interior, exterior, and other detection devices that are capable of:

1. Locating intrusions at individually protected asset areas or at an individual portal;

2. Locating intrusions within a specific area of coverage;

3. Locating failures or tampering of individual sensors or components.

B. Provide and adjust for devices so that coverage is maximized in the space or area it is installed in. For large rooms where multiple devices are required, ensure device coverage is overlapping.

C. Detection sensitivity shall be set up to ensure maximum coverage of the secure area is obtained while at the same time limiting excessive false alarms due to the environment and impact of small animals. All detection devices shall be anti-masking with exception of video motion detection.

D. Dual sensor technology shall be used when possible. Sensor technology shall not be of the same type that is easily defeated by a single method. This will reduce the amount of false alarms.

E. Interior Environmental Conditions: Systems shall be able to operate in environmentally protected interior areas and shall meet operational performance requirements for the following ambient conditions:

1. If components are installed in unheated areas they shall be able to operate in temperatures as low as -17 C (0 F);
2. Interior Sensor Environmental Characteristics:

Temperatures	0 to 50 C (32F to 120 F)
Pressure	Sea Level to 4573m (15,000 ft.) above sea level
Humidity	5% - 95%
Fungus	Components of non-fungus nutrient materials
Acoustical Noise	Suitable for high noise environments above 100db

F. Balanced Magnetic Switches (BMS)

1. BMS switches shall be surface or recessed mounted according to manufacturer's instructions. Recessed mounted is the preferred method to reduce tampering or defeating of the system. Switches shall activate when a disturbance in the balanced magnetic field occurs.
2. Switches shall have a minimum of two (2) encapsulated reed switches.
3. Contractor shall provide each BMS with a current protective device, rated to limit current to 80% of the switch capacity.
4. Surface Mounted BMS: For exterior application, components shall be housed in weatherproof enclosures.
5. BMS field adjustments in the fixed space between magnet and switch housing shall not be possible. Attempts to adjust or disturb the magnetic field shall cause a tamper alarm.
6. BMS Technical Characteristics:

Maximum current	.25 amperes
Maximum voltage	30 VDC
Maximum power	3.0 W (without internal terminating resistors). 1.0 W (with internal terminating resistors).

Components	Three (3) pre-adjusted reed switches Three (3) pre-adjusted magnets
Output contacts	Transfer type SPDT
Contact rating	0.5 amperes, 28 VDC
Switch mechanism	Internally adjustable ¼ - ½ in. (6-13 mm)
Wiring	Two (2) wires #22 American Wire Gauge (AWG), three (3) or 11 foot attached cable
Activation lifetime	1,000,000 activations
Enclosure	Nonferrous materials
Tamper alarm activation	Cover opened 3 mm (1/8 in.) and inaccessible until actuated

G. Window Intrusion Detection

1. These IDS devices shall detect intrusions thru inertia (shock) or by sound, and shall utilize either a Breakwire Sensor or Acoustic and Seismic Sensor.
2. Break wire Sensors (wire trap):
    a. Detect intrusion thru shock or breakage of window glazing. Also used for the protection of utility openings.
    b. Sensors shall consist of fine wire embedded in or affixed to interior of glazing. Breakage of protected glazing shall result in wire breakage.
    c. Wire shall be hard-drawn copper up to #26 AWG diameter.
    d. If sensors are affixed to glazing the sensor shall be protected by a clear coating which shall not affect sensor functioning.
    e. Sensor shall be terminated in insulated connectors which are concealed and tamper resistant.
    f. Protection of inlet openings:
        1) Shall consist of up to 26 AWG hard-drawn copper wire with a tensile strength of 17.8 N 4 pounds maximum.
        2) Wire shall be interlaced throughout the opening such that no opening between wires shall be larger than 100 mm (4 in.. on center.
        3) Sensors shall be terminated so that attempts to cut the wire or otherwise enlarge openings between wires shall cause an alarm.
        4) Sensors shall be terminated in insulated connectors which are concealed and tamper resistant.

H. Acoustic and Seismic Glass Break Detectors

1. Detects intrusion thru the use of audible sound and vibration emitted from the breaking of glass using a tuned frequency range and sound pattern recognition. This initiates an alarm when glass they protect is broken or cracked.
2. Detectors shall be installed in strict conformance with manufacture's installation instructions.
3. The detector's power circuit shall be switched via an output relay on the control panel to provide latching alarm LED reset capability.
4. Sensors shall be contained in a fire-resistant ABS plastic housing and must be mounted in contact with a window.
5. Sensing shall be accomplished through the use of a mechanical filtered piezoelectric element.
6. Sensors shall have a sensitivity adjustment controlling output voltage from the piezoelectric element which triggers a solid-state latching device.
7. Sensors shall selectively filter input to minimize false alarms and not initiate alarm in response to ambient seismic vibrations or other ambient stimuli.
8. A manufacturer's test unit will be used to validate the sensor by simulating glass breakage.
9. The Contractor shall provide sensors for adjusting sensitivity and two-sided polyurethane tape with acrylic adhesive for window attachment.
10. Sensor shall include exterior label to protect adhesive tape from direct sunlight.
11. Window Intrusion Detection Sensor Technical Specifications:

Power	Auxiliary power supply 12 VDC @ 25 mA (+/-) 10%
Power Input	10 – 15 VDC at 16mA protected against reverse polarity, 20 mA during relay closure
Relay Output Rating	Minimum of 25 VDC mA
Coverage Audio	6,000 Square ft.
Coverage Glass Break	7.5 m (25 ft.) wide by 7.5 m wide (25 ft.) Minimum: 7.62 m (25 feet) from the detector to the furthest point on protected glass.
Audio Output	300 – 12,000 HZ
Alarm Output	Relay NO or NC selectable
Interconnection	12 pin Panduit connector, 22 AWG
Radio Frequency Interface	No alarm or setup on between frequencies 26 – 100 MHz 50 v/m Immunity to mobile RF interference 100 watts 3 m @ (9.8 Ft.) in 27-100 MHz range
Alarm period	Two (2) to three (3)

Mounting	Ceiling, same wall, adjacent wall, opposite wall
Features	Test and alarm LEDs for acoustic seismic and alarm condition latching, Alarm LED and tamper switch on cover.
Alarm verification	Digital signal processing or dual acoustic processing technologies
Detection ability	Single and multi-pane glass, wired glass, tempered and laminated glass to 6 mm (¼ inch) or thickness

I. Screening

1. This material shall be used on windows to protect and detect intrusion as follows.
    a. Security screens shall be constructed from a maximum of 26 AWG insulated hard-drawn copper.
    b. Screens shall be connected to an alarm circuitry by means of flexible armored cords. Security screen circuitry shall provide end-of-line resistors in series or equivalent methods ensuring alarm activation if short-circuiting of the screen is attempted.
    c. If unable to install a break wire sensor (wire traps), then tamper switches will be provided.
    d. Contractor shall provide tamper switches in the frames as required with not less than one (1) switch on each side if dimensions are 610 mm two ((2) ft. square) or less, and two (2) switches if dimensions exceed 610 mm (2 ft. square). Tamper switches shall be corrosion-resistant, spring-operated, and shall initiate an alarm with a movement of 50 mm (two (2) in.) or less before access to the switch is possible.
    e. Electrical characteristics of the switch shall match the alarm system requirements.

J. Vibration Sensors

1. These sensors shall initiate alarms upon detecting drilling, cutting, or blasting through walls, or other methods of forced entry through a structure as follows.
2. Sensors shall detect and selectively amplify signals generated by forced penetration of a protective structure.
3. Sensors shall be designed to give peak response to structurally conveyed vibrations associated with forcible attack on the protected surface.
4. Sensors will initiate an alarm if attempts are made to remove them from the surface of the wall.
5. Sensors shall be enclosed in protective mountings.
6. Sensors shall include an adjustable alarm discriminator to prevent incidental vibrations which may occur from triggering the alarm circuit.
7. Sensors shall be provided with a tamper switch.
8. Sensor sensitivity shall be individually adjustable unless a sensor is designed to accommodate vibration ranges of specific surface type on which it will be mounted. Sensitivity adjustments shall not be accessible without removing the sensor cover. Also, a sensor shall not be responsive to airborne sound.

9. Vibration Sensor Technical Characteristics:

Power requirements	External DC power source Eight (8)- 14.5 VDC, two (2) volt max peak to peak ripple
Alarm output	Form C (NO/C/NC) solid state alarm relay, rated 100 mA, 28 VDC
Tamper Connection	Tamper switch and external magnetic
Current rating and alarm output	No alarm state 20mA SPDT relay contact rating (Form C)
Sensor range	Concrete (poured) 4 m (13.2 ft.) Concrete block 2 m (6.6 ft.) Brick block 1 m (3.3 ft.)
Frequency range	3kHz-20kHz (-15db) 7kHz-10kHz (-10db)
Adjustable	Sensitivity eight (8) steps Alarm response 0-30 sec

K. Passive Infrared Motion Sensors (PIR)

1. These sensors shall detect an intruder presence by monitoring the level of infrared energy emitted by objects within a protected zone and meet ANSI PIR-01 Passive Infrared Motion Detector Standards Features for Enhancing False Alarm Immunity. An alarm shall be initiated when motion and temperature changes within set patterns are detected as follows.
2. The detector shall provide multiple detection zones distributed at a variety of angles and distance.
3. Sensors shall be passive in nature; no transmitted energy shall be required for detection.
4. Sensors shall be sensitive to infrared energy emitted at wavelengths corresponding to human body and other objects at ambient temperatures.
5. Sensors shall not alarm in response to general area thermal variations and shall be immune to radio frequency interference.
6. Sensors shall not be susceptible to changes in temperature due to an air conditioner being turned on or off.
7. Sensors shall be housed in a tamper-alarmed enclosure.
8. Sensor detectors shall include motion analyzer processing, adjustable lens, and walk test LED’s visible from any angle.
9. Sensors shall provide some means of indicating an alarm condition during installation and calibration. A means of disabling the indication shall be provided within the sensor enclosure.
10. Sensor detectors shall include a motion monitoring verification circuit that will signal trouble or alarm if the detector fails to detect motion for an extended period.

11. PIR Technical Characteristics:

Power	Six (6) – 12 VDC 25 mA continuous current draw 38 mA peaks
Alarm Velocity	1500 mm (Five (5) ft.) at a velocity of 30 mm (0.1 ft.) per second, and one (1) step per second, assuming 150 mm (6 in.) per step. Also, faster than 30 mm (1 foot) per second, up to 3000 mm (10 feet) per second
Maximum detection range	10.6 m (35 ft.)
Frequency range- non activation or setup use	26 to 950 MHz using a 50 watt transmitter located 1 ft. from the unit or attached wiring
Infrared detection	1 1/2°C (3°F) different from the background temperature
Detection Pattern	180 degrees for volumetric units, non PIR 360
PIR 360°Detection Pattern	Programmable 60 detection zones including one directly below
Mounting	Ceiling and walls
Ceiling heights	2.4 m (Eight (8) ft.) – 5.4 m (18 ft)
Sensitivity adjustments	Three (3) levels

L. Microwave-Passive Infrared Detector

1. This sensor shall be designed to detect the motion of a human body within a protected area by means of a combination of microwave sensing technology and passive infrared (MPIR) sensing technology as follows.
2. The sensor shall require both technologies to sense intrusion before an alarm may occur.
3. The sensor shall be designed for wall mounting on swivel bracket. A high-security gimbaled bracket shall be provided.
4. The PIR fields of view shall be focused on the pyroelectric element by means of an internal multi-faceted mirror.
5. The sensor shall incorporate a look-down lens system that detects the passing of an intruder directly beneath the sensor.
6. The sensor shall incorporate a microwave supervision system which shall activate the trouble output if the device technology fails.
7. The sensor shall incorporate self-diagnostics which shall monitor the sensor systems and report a trouble to the control panel if any system device fails.

8. The sensor shall have compensation against loss of sensitivity as the ambient temperature nears human body temperature.

9. MPIR Technical Characteristics:

Technology	Microwave and Passive Infrared
Power	Nine (9) – 15 VDC max current consumption 22 mA at 12 VDC
Operating Temperature	0° C (32°F) – 49° C (120° F)
Detection Area	30 m (98 ft.) long by 3 m (9.8 ft.) wide or 21 m (69 ft.) long by 21m (69 ft.) wide
Electronics	Microcontroller based
Alarm Contact	Form-C rated 125 mA, 28 VDC
Tamper Contact	125 mA, 28 VDC
Trouble Contact	Form-B rated 25 mA, 30 VDC
Microwave Operating Frequency	10.525 GHz
Microwave Sensitivity	Adjustable on circuit board
Detection pattern adjustment	Changing of internal lens
Sensing element	Pyro-electric
LED Indicators	PIR, microwave, alarm
Bug and Dust protection	zero-clearance, gasket bug guard
Lens	Interchangeable: standard 18x24 m (60x80 ft.), corner mounting, ultra-wide, pet alley, long range, room and corridor combo, room and ceiling combo, creep zone

M. Photoelectric Sensors

1. The sensor devices shall be able to detect an intruder presence by sending out a series of infrared or ultraviolet beams. Intrusion is based on disruption of the signal beams as follows.
   a. Sensors shall consist of a modulating transmitter, focusing lenses, mirrors, demodulating receiver, power supply, and interconnecting lines.
   b. Beam transmitters shall be designed to emit light. Beams may be reflected by one (1) or more mirrors before being received and amplified.
   c. The photoelectric sensor shall initiate an alarm when the beam is interrupted with monitoring controls set at midrange.
   d. Transmitted beams shall be uniquely modulated to prohibit defeat of the IDS system by shining another light source into the receiver.

e. Sensors shall provide a means of local alarm indication on the detector for use at the protected zone during installation and calibration.

f. Sensors shall include an indicator-disabling device within the sensor enclosure.

g. Sensors shall utilize automatic gain control or be provided with sensitivity adjustments to allow for various beam lengths.

h. Sensor controls shall be inaccessible to operating personnel.

i. Sensors that use multiple beams shall be tested by attempting to crawl under and jump through and over beams. Each system sensor shall provide cutoffs of at least 90% to handle a high percentage of light cutoffs prior to initiating an alarm.

j. Sensor components shall be housed in tamper-alarmed enclosure.

2. Photoelectric Sensor Technical Characteristics:

Power requirements	Nine (9)-16 VDC, protected against reverse polarity
Relay output	Normally closed. 18 ohm resister in series with contacts. 0.5 amperes resistance/24 VDC
Current	Transmitter 15 mA, Receiver 15 mA
LED	Alignment, walk-test alarm, off
Range	Indoor: 39 m (130 ft.) Outdoor19.5 m: (65 ft.)
Alarm relay contacts	Two (2) amperes at 120 VAC minimum
Enclosure	High impact acrylic
Type	Dual beam
Mounting	Wall, corner, flush
Beam width	Six (6) degrees
Receiver field of view	Six (6) degrees horizontal and vertical
Adjustments	Vertical +10 – 20 degrees Horizontal 30 degrees
Alarm period	Two (2) – three (3) sec
Infrared source	Long-life Gallium Arsenide LED
Infrared sensor	PIN photodiode
Transmitter Frequency	One (1) kHz 10 microsecond pulse width
IR Wavelength	950 nm

N. CCTV Video Motion Detection Sensors: Refer to Section 28 23 00 VIDEO SURVEILLANCE that outlines related video motion detection requirements.

2.10 TAMPER ALARM SWITCHES

A. The following IDS sensors shall be used to monitor and detect potential tampering of sensors, control panels and enclosures.

   1. Tamper Switches: All enclosures including cabinets, housings, boxes, raceways, and fittings with hinged doors or removable covers containing circuits and power supplies related to the IDS shall include corrosion-resistant tamper switches.
   2. Tamper alarms shall be annunciated to be clearly distinguishable from IDS alarms.
   3. Tamper switches will not be in a viewable from a direct line of sight perspective. The minimum amount of time the tamper switch becomes active and sends a signal after an enclosure is opened or panel removable is attempted, shall be one (1) second.
   4. Tamper switches will initiate when enclosure doors or covers is removed as little as 6.35 mm (1/4 inch) from the closed position unless otherwise indicated. Tamper switches shall be:
      a. Push/pull automatic reset type;
      b. Inaccessible until switch is activated;
      c. Spring-loaded and held in closed position by door or cover; and
      d. Wired to break a circuit when door or cover is removed with each sensor annunciated individually at a central reporting processor.
   5. Fail-Safe Mode: Shall provide the capability to detect and annunciate diminished functional capabilities and perform self-tests. Fail-safe alarms shall be annunciated to be clearly distinguishable from other types of alarms.

2.11 POWER SUPPLY

A. A power supply shall only be utilized if the control panel is unable to support the load requirements of the IDS system.

B. All power supplies shall be UL rated and able to adequately power two entry control devices on a continuous base without failure.

C. Power supplies shall meet the following minimum technical characteristics:

INPUT POWER	110 VAC 60 HZ 2 amp
OUTPUT VOLTAGE	12 VDC Nominal (13.8 VDC) 24 VDC Nominal (27.6 VDC) Filtered and Regulated
BATTERY	Dependant on Output Voltage shall provide up to [insert number]Ah, rechargeable
OUTPUT CURRENT	4 amp max. @ 13.8 VDC 3 amp max. @ 27.6 VDC
BATTERY FUSE SIZE	3.5 A @ 250 VAC

CHARGING CIRCUIT	Built-in standard

2.12 AUDIBLE AND VISUAL ALARM DEVICES

A. Bell: Central-station control unit 10 inches (254 mm) in diameter, rated to produce a minimum sound output of 84 dB at 10 feet (3 m) from central-station control unit.

  1. Enclosure: Weather-resistant steel box equipped with tamper switches on cover and on back of box.

B. Weatherproof Motor-Driven Hooter: UL listed, rated to produce a minimum sound output of 120 dB at 3 feet (1 m), plus or minus 3 dB, at a frequency of 470 Hz. Rated for intermittent use: two minutes on and five minutes off.

  2. Designed for use in industrial areas and in high noise, severe weather marine environments.

C. Siren: 30-W speaker with siren driver, rated to produce a minimum sound output of 103 dB at 10 feet (3 m) from central-station control unit.

  3. Enclosure: Weather-resistant steel box with tamper switches on cover and on back of box.

D. Strobe: Xenon light complying with UL 1638, with a clear polycarbonate lens.

  4. Light Output: 115 cd, minimum.

  5. Flash Rate: 60 per minute.

2.13 SECURITY FASTENERS

Security fasteners shall be operable only by tools produced for use on specific type of fastener by fastener manufacturer or other licensed fabricator. Drive system type, head style, material, and protective coating as required for assembly, installation, and strength.

SPEC WRITER NOTE: Insert additional types of security fasteners below with other drive systems and head styles if necessary or for special applications. Coordinate type of security fasteners retained in this Section with other Sections specifying security fasteners. See Evaluations.

A. Drive System Types: Pinned Torx or pinned hex (Allen).

B. Socket Flat Countersunk Head Fasteners:

  1. Heat-treated alloy steel, ASTM F 835 (ASTM F 835M).

  2. Stainless steel, ASTM F 879 (ASTM F 879M), Group 1 CW.

C. Socket Button Head Fasteners:

  1. Heat-treated alloy steel, ASTM F 835 (ASTM F 835M).

  2. Stainless steel, ASTM F 879 (ASTM F 879M), Group 1 CW.

D. Socket Head Cap Fasteners:

  1. Heat-treated alloy steel, ASTM A 574 (ASTM A 574M).

  2. Stainless steel, ASTM F 837 (ASTM F 837M), Group 1 CW.

E. Protective Coatings for Heat-Treated Alloy Steel:

1. Zinc chromate, ASTM F 1135, Grade 3 or 4; for exterior applications and interior applications where indicated.
2. Zinc phosphate with oil, ASTM F 1137, Grade I, or black oxide.

3 PART 3 - EXECUTION

SPEC WRITER NOTE: Delete and/or amend this all paragraphs and sub-paragraphs to apply to only the equipment and devices that are being installed.

3.1 INSTALLATION

A. IDS installation shall be in accordance with Underwriters Laboratories (UL) 639 Standards for Intrusion Detection Units and UL 634 Standards for Connectors with Burglar Alarm Systems, and appropriate manufacture's installation manuals for each type of IDS.

B. Components shall be configured with appropriate "service points" to pinpoint system trouble in less than 30 minutes.

C. The Contractor shall install all system components including City of Austin furnished equipment, and appurtenances in accordance with the manufacturer's instructions and shall furnish all necessary connectors, terminators, interconnections, services, and adjustments required for a complete and operable system.

D. The IDS will be designed, engineered, installed, and tested to ensure all components are fully compatible as a system and can be integrated with all associated security subsystems, whether the system is a stand-alone or designed as a computer network.

E. The IDS shall be able to be integrated with other security subsystems. Integration with these security subsystems shall be achieved by computer programming and the direct hardwiring of the systems. Determination for methodology shall be outlined when the system(s) is/are being designed and engineered. For installation purposes, the IDS shall utilize an output module for integration with other security subsystems. The Contractor will ensure all connections are per the OEM and that any and all software upgrades required to integrate the systems are installed prior to system start-up.

F. For programming purposes, the Contractor shall refer to the manufacturer's requirements and Contracting Officer instructions for correct system operations. This includes ensuring computers being utilized for system integration meet or exceeds the minimum system requirements outlined in the IDS software packages.

G. Lightening and power surges to the central alarm reporting and display unit shall be protected at both ends against excessive voltages. This requirement shall apply for circuits that are routed both in underground conduits and overhead runs.

H. At a minimum, the Contractor shall install primary detection devices, such as three electrode gas-type surge arresters, and secondary protectors to reduce dangerous voltages to levels that will cause no damage. Fuses shall not be permitted as protection devices.

I. The Contractor shall provide fail-safe gas tube type surge arresters on exposed IDS data circuits. In addition, transient protection shall protect against spikes up to 1000 volts peak voltage with a one-microsecond rise time and 100-microsecond decay time, without causing false alarms. The protective device shall be automatic and self-restoring. Also, circuits shall be designed or selected assuming a maximum of 25 ohms to ground.

J. Product Delivery, Storage and Handling:

1. Delivery: Deliver materials to the job site in OEM's original unopened containers, clearly labeled with the OEM's name, equipment model and serial identification numbers, and UL logo. The Contracting Officer may inventory the IDS equipment at the time of delivery and reject items that do not conform to this requirement.
2. Storage and Handling: Store and protect equipment in a manner that will preclude damage as directed by the Contracting Officer.

K. Cleaning and Adjustments:

1. Cleaning: Subsequent to installation, clean each system component of dust, dirt, grease, or oil incurred during installation in accordance to manufacture instructions.
2. Prepare for system activation by following manufacturer's recommended procedures for adjustment, alignment, or synchronization. Prepare each component in accordance with appropriate provisions of the component's installation, operations, and maintenance instructions.

L. Tamper Switches

1. Install tamper switches to initiate an alarm signal when a panel, box, or component housing door or cover is moved as little as 6.35 mm (1/4 inch) from the normally closed position unless otherwise specified.
2. Locate tamper switches within enclosures, cabinets, housings, boxes, raceways, and fittings to prevent direct line of sight to any internal components and to prevent tampering with switch or circuitry.
3. Conceal tamper switch mounting hardware so that the location of the switch within the enclosure cannot be determined from the exterior.

M. Unique IDS Installation Components:

1. BMS Surface Mounted:

   a. Surface mounted BMS housing for the switch element shall have the capability to receive threaded conduit. Housing covers for surface mounted BMS, if made of cast aluminum, shall be secured by stainless steel screws. Magnet housing cover shall not be readily removable and BMS housings shall be protected from unauthorized access by a cover operated, corrosion-resistant tamper device.

   b. Conductors running from a door to alarm circuits shall be contained within a flexible armored cord constructed from corrosion-resistant metal. Each end of the armored cord shall terminate in a junction box or other enclosure. Armored cord ends shall be mechanically secured to the junction boxes by clamps or bushings. Conductors within the armored cord shall be provided with lug terminals at each end. Conductors and the armored cord shall experience no mechanical strain as the door is removed from fully open to closed position. Switch circuits shall initiate an alarm if a short circuit is applied to the door cord.

   c. For exterior application on double gates, both BMS elements must be mounted on the gate. Flexible armored cord constructed from corrosion-resistant metal shall be used to provide electrical connection.

2. BMS Recessed Mounted:

   a. Ball bearing door trips shall be mounted within vault door headers such that when the locking mechanism is secured, the door bolt engages an actuator, mechanically closing the switch.

   b. Door bolt locking mechanisms shall be fully engaged before the ball bearing door trip is activated. Also, circuit jumpers from the door shall be provided.

3. Vibration Sensors:

   a. Mount vibration sensors directly contacting the surface to be protected.

   b. Provide at least one (1) sensor on each monolithic slab or wall section, even though spacing closer than that required for midrange sensitivity may result.

   c. House sensors in protective mountings and fasten to surface with concealed mounting screws or an epoxy.

   d. Adjust discriminator on the job to precise needs of application. Connect sensors to an electronic control unit by means of wiring or fiber optics cable run in rigid steel conduit or electrical metallic tubing (EMT).

4. Passive Infrared Detectors: (PIR)

   a. The protective beam shall be focused in a straight line.

   b. Installed beam distance from transmitter to receiver shall not exceed 80% of the manufacturer's maximum recommended rating.

   c. Mirrors may be used to extend the beam or to establish a network of beams. Each mirror used shall not lower the rated maximum system range by more than 50%.

   d. Mirrors and photoelectric sources used in outdoor applications shall have self-heating capability to eliminate condensation and shall be housed in weatherproof enclosures.

5. Taut-Wire:

   a. Housing for switch assembly shall be covered by a neoprene cap to retain the center bolt (lever arm), which functions as a lever to translate movement of the attached horizontal wire into contact closure. When the neoprene cap is firmly seated on the cup-shaped polycarbonate housing, it shall function as the fulcrum for the lever (bolt).

   b. Upper exposed end of the lever shall be threaded to accommodate clamping to the horizontal wire. The lower end of the lever, which is fashioned to serve as the movable electrical contact, shall be held suspended in a small cup-shaped contact that floats in a plastic putty material.

   c. Plastic putty used shall retain a degree of elasticity under varying temperature conditions and provide the sensor switch with a self-adjusting property. This provides the switch with a built-in compensating mechanism that ignores small, very slow changes in lever alignment (i.e. which may result from environmental changes such as extreme temperature variations and ground seepage due to weather conditions) and to react to fast changes only, as caused by manual deflection or cutting of the wires.

   d. Contractor shall provide metal slider strips having slots through which the barbed wires pass. Wires shall be prevented from leaving the slots by rivets. A slider strip shall be used to translate normal forces to the barbed wire and to the horizontal displacement of the sensor.
   e. Install one (1) slider strip pair, upper and lower, on every fence post except where sensor posts or anchor strips are installed.
   f. Separation between slider elements along the fence shall be 3000 mm (10 feet).
   g. Attach wires of sensor to existing, specially installed fence posts, called anchor posts, located equidistant on both sides of sensor posts and at ends of sensor zone run.
   h. Anchor strip shall be a strip of steel plate on which fastening plates are installed. Weld or otherwise attach the strip to anchor post and ends of tensed barbed wires wrapped around the fastening plates. Attempts to climb on fastening plates or on the attached barbed wires shall cause plates to break off, creating an alarm and making it impossible to defeat the system by climbing at the anchor post.
   i. The use of barbed wire as part of the IDS system shall be suitable for installation under a preload tension of approximately 392 N 88 pounds and be flexible enough for convenient manipulation during tensioning. Double-strand 15 1/2-gage barbed wire shall be the minimum acceptable.
6. Electromechanical Fence Sensors:
   a. The fence length shall be divided into 100m (300 ft). or zones.
   b. Sensors shall consist of individual electromechanical sensing units mounted every three-thousand and 3045mm (10 ft). on the fence fabric or posts and wired in series to a sensor zone control unit and associated power supply.
7. Electrostatic Field Sensors:
   a. Sensors shall be capable of following irregular contours and barrier bends without degrading sensitivity below the specified detection level.
   b. In no case shall a single sensor zone exceed 100m (300 ft). or be long enough to significantly degrade sensitivity.
   c. Adjacent zones shall provide continuous coverage to avoid a dead zone. Adjacent zones shall be designed to prevent crosstalk interference.
   d. Exterior components shall be housed in rugged corrosion-resistant enclosures, protected from environmental degradation and include tamper switches.
   e. Interfacing between exterior units shall be carried in underground cables.
   f. Exterior support hardware shall be stainless or galvanized to avoid tension degradation.
   g. Sensor and field wires shall be stainless steel. Wire spacing for various configurations shall be maintained constant throughout each zone and shall be uniform with respect to the ground and follow manufacturer's specifications.
   h. Signal processing equipment shall be separately mounted such that no desensitized zones are created within the zone of detection.
8. Microwave: Do not install microwave sensors where fluorescent lights may pose a problem due to radiated ionization from lights.

3.2 WIRING INSTALLATION

SPECS WRITER NOTE: Coordinate this Article with Drawings. Select one of first three paragraphs below to specify wiring method. Retain/Delete first two paragraphs and retain and revise third paragraph to suit Project.

A. Wiring Method: Install wiring in metal raceways according to Section 28 05 28.33 "CONDUITS AND BOXES FOR ELECTRONIC SAFETY AND SECURITY." Conceal raceway except in unfinished spaces and as indicated. Minimum conduit size shall be 3/4 inch (20 mm). Control and data transmission wiring shall not share conduit with other building wiring systems.

B. Wiring Method: Install wiring in raceways except in accessible indoor ceiling spaces and in interior hollow gypsum board partitions where cable may be used. Conceal raceways and wiring except in unfinished spaces and as indicated. Minimum conduit size shall be 3/4 inch (20 mm). Control and data transmission wiring shall not share conduit with other building wiring systems.

C. Wiring Method: Cable, concealed in accessible ceilings, walls, and floors when possible.

D. Wiring within Enclosures: Bundle, lace, and train conductors to terminal points. Use lacing bars and distribution spools. Separate power-limited and non-power-limited conductors as recommended in writing by manufacturer. Install conductors parallel with or at right angles to sides and back of enclosure. Connect conductors that are terminated, spliced, or interrupted in any enclosure associated with intrusion system to terminal blocks. Mark each terminal according to system's wiring diagrams. Make all connections with approved crimp-on terminal spade lugs, pressure-type terminal blocks, or plug connectors.

E. Wires and Cables:

SPECS WRITER NOTE: Coordinate subparagraphs below with Drawings.

1. Conductors: Size as recommended in writing by system manufacturer, unless otherwise indicated.
2. 120-V Power Wiring: Install according to Division 26 Section "LOW-VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES," unless otherwise indicated.
3. Control and Signal Transmission Conductors: Install unshielded, twisted-pair cable, unless otherwise indicated or if manufacturer recommends shielded cable, according to Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."
4. Computer and Data-Processing Cables: Install according to Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."
5. Television Signal Transmission Cables: Install according to Division 28 Section "CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY."

F. Splices, Taps, and Terminations: Make connections only on numbered terminal strips in junction, pull, and outlet boxes; terminal cabinets; and equipment enclosures.

G. Install power supplies and other auxiliary components for detection devices at controllers, unless otherwise indicated or required by manufacturer. Do not install such items near devices they serve.

H. Identify components with engraved, laminated-plastic or metal nameplate for central-station control unit and each terminal cabinet, mounted with corrosion-resistant screws.

3.3 GROUNDING

A. Ground system components and conductor and cable shields to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

B. Signal Ground Terminal: Locate at main equipment rack or cabinet. Isolate from power system and equipment grounding. Provide [5] <Insert selected maximum value>-ohm ground. Measure, record, and report ground resistance.

SPEC WRITER NOTE: Coordinate paragraph below with Drawings.

C. Install grounding electrodes of type, size, location, and quantity indicated. Comply with installation requirements in Division 28 Section "GROUNDING AND BONDING FOR ELECTRONIC SAFETY AND SECURITY SYSTEMS."

3.4 STARTUP AND TESTING

A. The Commissioning Agent will observe startup and contractor testing of selected equipment. Coordinate the startup and contractor testing schedules with the Resident Engineer and Commissioning Agent. Provide a minimum of 7 days prior notice.

3.5 COMMISSIONING

A. Provide commissioning documentation in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS for all inspection, start up, and contractor testing required above and required by the System Readiness Checklist provided by the Commissioning Agent.

B. Components provided under this section of the specification will be tested as part of a larger system. Refer to Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS and related sections for contractor responsibilities for system commissioning.

3.6 TESTS AND TRAINING

SPECS WRITER NOTE: Edit text below per project requirements.

A. All testing and training shall be compliant with the City of Austin General Requirements, Section 01 00 00, GENERAL REQUIREMENTS.

B. Provide services of manufacturer’s technical representative for [insert number] hours to instruct City of Austin personnel in operation and maintenance of units.

C. Submit training plans and instructor qualifications in accordance with the requirements of Section 28 08 00 – COMMISSIONING OF ELECTRONIC SAFETY AND SECURITY SYSTEMS.

-----END----

28 23 00 VIDEO SURVEILLANCE FOR ELECTRONIC SAFETY AND SECURITY

COMMUNICATIONS & TECHNOLOGY MANAGEMENT

ENTERPRISE ELECTRONIC SECURITY SYSTEM (ESS) SPECIFICATIONS

Version 1.0, City of Austin, Texas

January, 2014

1 PART 1 - GENERAL

1.1 DESCRIPTION

A. Equipment and materials used shall be standard components that are manufactured and available for purchase as standard replacement parts as long as the product is commercially available from the manufacturer.

B. All manufactured products shall be thoroughly tested and proven in actual use.

C. All manufactured products shall include, at no additional cost, online support services and availability of a toll-free (U.S. and Canada), 24-hour technical assistance program (TAP) for emergencies.

D. The manufacturer shall repair or replace without charge, manufactured products proven defective in material or workmanship for the stated warranty period from the date of shipment.

2 PART 2 - PRODUCTS

2.1 GENERAL

A. Equipment and materials used shall be standard components that are manufactured and available for purchase as standard replacement parts as long as the product is commercially available from the manufacturer.

B. All manufactured products shall be thoroughly tested and proven in actual use.

C. All manufactured products shall include, at no additional cost, online support services and availability of a toll-free (U.S. and Canada), 24-hour technical assistance program (TAP) for emergencies.

D. The manufacturer shall repair or replace without charge, manufactured products proven defective in material or workmanship for the stated warranty period from the date of shipment.

2.2 IP VIDEO MANAGEMENT SYSTEM

A. The IP video management system shall consist of Digital Sentry® NVs version 7 software operating on an optimized Pelco-supplied hardware platform. The NVs software shall consist of base software with individual, non-expiring licenses in the required quantity.

B. The IP video management system software updates shall be downloadable from a publicly available website.

C. The IP video management system shall support up to 128 combined IP and analog video streams, with up to 64 direct-attached analog cameras. Analog streams shall be supported using Pelco and/or third-party encoders.

D. The IP video management system shall provide 280 Mbps throughput for recording of analog and IP video streams, playback and export.

E. The IP video management system shall support recording of JPEG, MPEG-4 and H.264 IP streams.

F. The IP video management system shall support Pelco and third-party H.264 Megapixel video streams up to 10 Megapixel resolution with quantities based on a total system of 280 Mbps throughput for recording of analog and IP video streams, playback and export.

G. The IP video management system shall have a fully open architecture with support for both IP-specific camera as well as cameras with ONIVIF compliance.

H. The IP video management system shall support automatic detection of Pelco IP cameras. Third-party IP cameras shall be automatically detected dependent on IP driver versions and manufacturers specifications.

I. The IP video management system shall support up to 64 looping analog camera inputs with direct-attached 16-channel encoders; up to four direct-attached units. The direct-attached 16-channel encoders shall support H.264 compression, CIF, 2CIF, and D1 resolutions at maximum 30ips, 16 audio inputs and RS422/485 PTZ control with Pelco P and D protocols.

J. The IP video management system shall support an unlimited number of systems connected over a network. Each system shall contain two 1GB network ports; one for IP camera/encoder data, and one to connect to a network for client computer access.

K. The IP video management system shall be viewed, managed, and played back through a single user interface simultaneously with other Digital Sentry digital video management systems through supplied DS Admin or DS ControlPoint Client software.

L. The IP video management system shall operate on a 2nd Generation Intel® Core™ i7 processor and 8 GB of RAM.

M. The IP video management system shall utilize a Windows® 7 Ultimate 64-bit operating system.

N. The IP video management system shall support and have an option for an internal DVD+/-RW.

O. The IP video management system shall contain two DVI-D ports.

P. The IP video management system shall allow expansion of IP video channel capacity through a licensing without any hardware modification.

Q. The IP video management system shall support multiple models of IP cameras and encoders including Pelco cameras and encoders with Sarix technology and multiple third-party manufacturers.

R. The IP video management system shall support audio recording from Pelco cameras with Sarix technology in addition to third-party manufacturer's audio recording.

S. The IP video management system shall support recording the internal server with additional storage utilizing SCSI attached Pelco DX8100-HDDI storage.

T. The IP video management system shall be capable of continuous scheduled alarm/event and motion recording. Pre- and post- alarm recording shall also be available and shall be fully programmable on a per channel basis.

U. The IP video management system shall allow archival of video data to computers or SAN storage devices over a network connection with the optional DS Archive Utility. The archival schedule shall be either automatic at user-defined intervals or manual and shall be configurable per connected camera.

V. The IP video management system shall support network health and monitoring utilizing third-party SNMP monitoring tools.

W. The IP video management system shall indicate system performance and operation status utilizing a variety of HTML reports.

X. The IP video management system shall display system health monitoring data utilizing front panel LED displays and display popups.

Y. The IP video management system shall optionally support on-board video analytics in quantities of two or four channels with Active Alert software and the DS DataPoint interface. The DS DataPoint interface shall provide video analytics monitoring including tracking and counting objects and people.

Z. The IP video management system shall support Lightweight Directory Access Protocol (LDAP).

AA. System Specifications

1. Hardware

Processor	2nd Generation Intel® Core™ i7
Internal Memory	8 GB RAM
Network	2 Gigabit Ethernet RJ-45 (1000Base-T)
User Interface	DS Control Point
Internal Storage	(JBOD or RAID 5)

DS-SRV	500 GB, 3 TB, 6 TB, 9 TB, 12 TB, or 18 TB
DS-SRV-DVD	500 GB, 3 TB, 6 TB, 9 TB, or 12 TB
Raid Level	RAID 5 (required optional DS-SRV-RAID
controller card)	
External Storage	Up to 24 TB JBOD or RAID 5 through
DX8100HDDI	
System Drives	
DS-SRV	6, 3.5-inch hard drive bays, hot swappable
PCI-E Slots	1 PCI-E x 16 and 1 PCI-E x 4
Auxiliary Interfaces	
USB Ports	1 front (USB 2.0), 4 rear (2 USB 3.0; 2 USB 2.0)
Power Input	100 to 240 VAC, 50/60 Hz, Autoranging

2. Environmental Specifications

Operating Temperature	10º to 35ºC (50º to 95ºF)
Operating Humidity	20% to 80%, noncondensing
Maximum Humidity	
Gradient	10% per hour
Operating Altitude	–15 to 3,048 m (–50 to 10,000 ft)
Operating Vibration	0.25 G at 3 Hz to 200 Hz at a rate of 0.5
octave/minute	
Dimensions	50.8 x 43.4 x 8.9 cm

3. Certifications

CE, Class A; meets EN50130-4 standard requirements

FCC, Class A

UL/cUL Listed

CCC

KCC

2.3 Video Management Software

A. IP Video Management Client Software requirements

1. The IP video management system shall provide the capability of running a client application in additional to the video management system.

2. A client computer with system compatible software shall be the user interface for viewing one or more systems. Live and recorded video and current event video shall be displayed on any client computer using a proper login and password. The client computer shall be able to connect to an unlimited number of recorders simultaneously to display live and recorded video.
3. Client Software shall be unlicensed and available to be installed on as many clients as required by the user.
4. Client Software shall be compatible with multiple DVR and NVR platforms to include all Pelco Digital Sentry®, Pelco DX8000/DX8100, and Pelco DX4100, DX4500/DX4600, DX4700/DX4800.
5. Client Software shall be password controlled such that password functionality set at each connected system will be recognized at the client. Password shall limit the ability to access live or recorded video as well as the ability to export video.
6. Client Software shall allow multiple monitor support for up to four displays per client workstation, providing virtual matrix functionality.
7. Client Software shall allow the connection of Pelco KBD5000 keyboard controllers to the client workstation to control PTZ operations and camera call-up.
8. Client Software shall allow video streams to be selectable from a system tree on an individual camera, individual system, client defined local groups, or from predefined recorder based groups.
9. Client Software shall be a tab based work environment with the ability to undock the tabs creating a virtual workspace on single or multiple monitor clients.
10. Client tabs shall include system management, live, and search options. Tabs can be displayed simultaneously on the client.
11. Systems Tab shall display and sort available systems, connection status, system names, system IP addresses, and custom categories. This tab shall additionally allow:
    a. Manual connect and disconnect of systems to the client
    b. Virtual systems naming
    c. Auto Connecting
    d. Adding, deleting, and editing available systems
    e. Live video tab shall have the ability to be created up to four times on a single client workstation providing for video display combinations and simultaneous video streams from as many different systems with consideration for maximum client bandwidth.
12. Live video tab shall provide the following functionalities:

   a. Quick Review which shall display recorded video from the last 1, 5, 15, 30, 60 or 90 minutes, providing near instantaneous review of recent events
   b. One week graphical display of recorded video
   c. Borderless display option
   d. Screen layout selection
   e. On the fly on-screen display changes including time, date, camera name, frame rate, frame size, alarm display, and border indicators
   f. Digital zoom
   g. User selectable in-video PTZ control or dashboard style control
   h. Drag and drop audio support associating any audio with any video

13. Search video tab shall allow for the search of one or multiple cameras from one or multiple systems simultaneously. Search tab shall provide the following functionalities:
    a. Time and date search
    b. Advanced data search with DataPoint interfaced software to Active Alert Intelligent Video and POS
    c. Drag and drop audio support to associate audio with any video
    d. Video export to any system accessible media including locally to HDD, CD/DVD, Flash USB device or to network storage
    e. Video authentication of exported video via check sum verification
14. Alarm video tab shall allow for alarm pop-up and playback of active alarms. Alarms may be based on motion activity, an external software trigger from Active Alert analytics or a preset data alarm from DS DataPoint. An alarm list pane shall be displayed for playback of queued alarms.
15. The Client shall incorporate virtual matrix functionality whereby camera sequences may be created on the monitoring workstation with the following functionalities:
16. Each sequence shall have a maximum of 500 cameras
17. Each camera in the sequence shall have its own individual dwell time, from 1 to 60 seconds
18. Each entry in a sequence shall have the capacity to trigger PTZ camera presets, patterns, or auxiliaries
19. The Client shall have the capability to display recorded video with full VCR controls. This feature shall display video from multiple cameras simultaneously. The user shall be able to play video as fast as possible (all images), in real time, or by skipping a selectable number of seconds

20. The Client shall support simultaneous playback of up to sixteen cameras all synchronized with each other. Non-synchronous playback of multiple cameras shall not be acceptable
21. The Client shall support tours of multi-camera displays
22. Remote Client Minimum PC Requirements

Processor	2nd Generation Intel® Core i7 processor with integrated graphics
Memory	4 GB or higher
Graphics Card	Graphics controller card with 512 MB (or greater) dedicated video memory
Operating System	Windows XP Professional SP2, Windows Vista (32 or 64 -bit), Windows 7 (32 or 64 bit)
Warranty	3 year parts and labor

23. Pelco Model Numbers – CCTVNVS System shall be sized such to provide the customer with 30-days of recording.

    DS-SRV-005

    DS-SRV-030

    DS-SRV-060

    DS-SRV-090

    DS-SRV-120

    DS-SRV-150

    DS-SRV-180

    DS-SRV-005DVD

    DS-SRV-030DVD

    DS-SRV-060DVD

    DS-SRV-090DVD

    DS-SRV-012DVD

    ENC5416 - Direct-attached analog encoder

To support the re-purposed cameras from the existing facility; the SMS contractor will provide the appropriate number of analog encoders to enable these cameras to be seamlessly integrated into the SMS system.

2.4 IM10LW-V SERIES SARIX® IP MINI DOME CAMERA

A. INDOOR/OUTDOOR, VANDAL-RESISTANT, 1.2 MEGAPIXEL NETWORK MINI DOME CAMERA

B. The network camera shall offer dual video streams with up to 1.2 megapixel resolution (1280 x 960) in progressive scan format.

C. The network camera shall provide SureVision technology which includes extended Wide Dynamic Range (WDR), low-light performance, and anti-bloom technology.

D. The network camera shall use a true WDR sensor that takes multiple exposures at the pixel level and has a rating for WDR of 120dB.

E. The network camera shall be a compact size with a 3-inch class bubble, shall include a rugged indoor enclosure, and an integrated varifocal 2.8~10 mm lens.

F. The network camera shall be capable of firmware upgrades through a network using a software-based device utility.

G. The network camera enclosure shall offer an impact resistance rating of IK10++ per EN62262 (50J). The enclosure shall also be vandal and tamper resistant.

H. The back box shall be plenum rated per 2008 NEC article 300.22(C) (2).

I. The network camera shall provide an accessory port for hardware expansion.

J. The network camera shall provide advanced low-light capabilities with sensitivity down to 0.0013 lux.

K. The network camera shall offer auto focus functionality.

L. The network camera shall provide a service connector to assist the installer when setting the field of view and focusing the camera.

M. The network camera shall provide line-in and line-out audio and built-in microphone.

N. The network camera shall support two simultaneous, configurable video streams. H.264 and MJPEG compression formats shall be available for primary and secondary streams with selectable Unicast and Multicast protocols. The streams shall be configurable in a variety of frame rates and bit rates.

O. The network camera (day/night model) shall have a removable IR cut filter mechanism for increased sensitivity in low-light installations. IR cut filter removal shall be configurable through a Web browser.

P. The network camera shall support industry standard Power over Ethernet (PoE), IEEE 802.3af, Class 2 to supply power to the camera over the network.

Q. The network camera shall use a standard Web browser interface for remote administration and configuration of camera parameters.

R. The network camera shall offer a video output port providing an NTSC/PAL analog video output signal for adjusting the field of view and when focusing the camera.

S. The network camera shall have a window blanking feature to conceal user-defined privacy areas that cannot be viewed by an operator. The network camera shall support up to four blanked windows. A blanked area shall appear on the screen as a solid gray window.

T. The network camera shall provide the Adaptive Motion analytic to intelligently detect motion within the field of view and trigger an alarm.

U. The network camera shall provide Camera Sabotage analytics to detect changes in the camera's field of view, including obstruction of the lens (examples include by cloth, spray paint, or a lens cap cover) and unauthorized movement of the camera. Such behaviors shall trigger an alarm.

V. The network camera shall support standard IP protocols.

W. The network camera shall support open architecture best practices with a published API available to third-party network video recording and management systems.

X. The network camera shall meet or exceed the following design and performance specifications.

Y. Camera Specifications

Imaging Device	1/3-inch, effective
Imager Type	CMOS
Imager Readout	Progressive scan
Maximum Resolution	1280 x 960
Signal-to-Noise Ratio	50 Db
Auto Iris Lens Type	DC drive
Electronic Shutter Range	1~1/77,000 sec
Wide Dynamic Range	Rated 120 dB at the sensor
White Balance Range	2,000° to 10,000°K
Sensitivity	f/1.2; 2,850ºK; SNR > 20 Db
Color (1x/33ms)	0.10 lux
Color SENS (15x/500ms)	0.005 lux
Mono (1x/33ms)	0.05 lux
Mono SENS (15x/500ms)	0.0013 lux
Dome Attenuation	
Clear dome	Zero light loss
Smoked dome	f/1.0 light loss
Construction	
Back box	Alodine aluminum
Bubble	Polycarbonate plastic

Finish Light gray powder coat

Weight 0.6 kg (1.4 lb)

Available Languages Chinese, English, French, German, Italian,

Portuguese, Russian, Spanish, and Turkish

Video Specifications

Video Encoding H.264 in Base profile and MJPEG

Video Streams Up to 2 simultaneous stream; the second stream

is variable based on the setup of the primary stream

Frame Rate Up to 30, 25, 24, 15, 12.5, 12, 10, 8, 7.5, 6, 5, 4, 3,2, and 1 (dependent upon coding, resolution, and stream configuration)

Available Resolutions

1.3 Mpxl 1280 x 1024; 5:4 aspect ratio; 20.0 ips max., 10.0 Mbps bit rate for MJPEG; 8.0 ips max., 2.5 Mbps bit rate for H.264

1.2 Mpxl1280 x 960; 4:3 aspect ratio; 20.0 ips max., 9.8 Mbps bit rate for MJPEG; 8.0 ips max., 2.4 Mbps bit rate for H.264 0.9 Mpxl1280 x 720; 16:9 aspect ratio; 30.0 ips max., 10.0 Mbps bit rate for MJPEG; 12.5 ips max., 2.5 Mbps bit rate for H.264 0.5 Mpxl 800 x 600; 4:3 aspect ratio; 30.0 ips max., 5.8 Mbps bit rate for MJPEG; 25.0 ips max., 2.0 Mbps bit rate for H.264 0.3 Mpxl 640 x 480; 4:3 aspect ratio; 30.0 ips max., 3.7 Mbps bit rate for MJPEG; 30.0 ips max., 1.6 Mbps bit rate for H.264 0.1 Mpxl 320 x 240; 4:3 aspect ratio; 30.0 ips max., 0.9 Mbps bit rate for MJPEG; 30.0 ips max.,0.4 Mbps bit rate for H.264

Additional640 x 512, 640 x 352, 480 x 368, 480 x 272, 320 x 256, 320 x 176

Supported Protocols TCP/IP, UDP/IP (Unicast, Multicast IGMP),

UPnP,DNS,DHCP, RTP, RTSP, NTP, IPv4, SNMP v2c/v3,QoS, HTTP, HTTPS, LDAP (client), SSH, SSL, SMTP,FTP, and 802.1x (EAP)

Users

Unicast - Up to 20 simultaneous users depending on resolution settings (2 guaranteed streams)

Multicast Unlimited H.264

Security Access Password protected

Software Interface Web browser view and setup

Pelco System Integration Endura® 2.0 (or later) Digital Sentry® 4.3 (or later)

Open IP Integration Pelco IP camera API

Minimum PC Requirements

Processor Intel® Pentium® 4 microprocessor, 1.6 GHz

Operating System Microsoft® Windows® XP, Windows Vista®, or Mac OS® X 10.4 (or later)

Memory 512 MB RAM

Network Interface Card 100 Mbps or greater

Monitor Minimum of 1024 x 768 resolution, 16- or 32-bit pixel color resolution

Web Browser Internet Explorer® 7.0 (or later); Mozilla® Firefox® 3.5 (or later); Internet Explorer® 8.0 (or later) is recommended for configuring analytics Media Player Pelco Media Player or QuickTime® 7.6.5 for Microsoft Windows XP, Windows Vista, or QuickTime 7.6.4 for Mac OS X 10.4

Electrical Specifications

Port	RJ-45 for 100Base-TX, Auto MDI/MDI-X
Cable Type	Cat5 cable or better for 100Base-TX
Power Input	PoE (IEEE802.3af class 2)
Power Consumption	3.9 W nominal
Service Port	External 3-connector, 2.5 mm provides NTSC/PAL video output
Accessory Port	Connects Pelco accessories
Audio	
Streaming	Bi-directional, full or half duplex
Input/output	Line level/ external microphone input; 600-ohm differential, 1 Vp-p max signal level; built-in microphone
Compression	G.711 PCM 8 bit, 8 kHz mono at 64 Kbit/s

Environmental Specifications

Operational Temperature	0° to 50°C (32° to 122°F)
Operational Humidity	20% to 80%, noncondensing
Impact Resistance	IK10++ per EN62262 (50J)
Shock and Vibration	Meets EN50155 Category 1, Class B; IEC60068: 2-6 and 2-27

Mechanical Specifications

Pan/Tilt Adjustment	Manual
Pan	355°
Tilt	180°
Rotate	220°

Certifications

CE, Class A

FCC, Class A

UL/cUL Listed

C-Tick

KCC

Meets NEMA Type 4 and IP56 standards

Warranty

36 months, parts and labor

Pelco Model Numbers

IM10LW10-1V	Sarix vandal-resistant, indoor fixed IP mini dome camera with SureVision, 1.2 Mpxl, low-light, WDR, day/night, 2.8~10mm varifocal megapixel lens, clear dome

2.5 SPECTRA® HD SERIES NETWORK DOME POSITIONING SYSTEM

A. INDOOR / OUTDOOR CAMERA DOME POSITIONING SYSTEM

B. The indoor/outdoor camera dome system shall provide a 100Base-TX network interface for live streaming to a standard Web browser.

C. The indoor/outdoor camera dome system shall be a discreet camera dome system consisting of a dome drive with a variable speed/high speed pan/tilt drive unit with continuous 360° rotation; 1/4-inch high resolution color, monochrome, or color/black-white CCD camera; motorized zoom lens with optical and digital zoom; auto focus; and an enclosure consisting of a back box, lower dome, and a quick-install mounting.

D. The indoor/outdoor network positioning camera shall support standard IT protocols.

E. The indoor/outdoor network positioning camera shall use a standard Web browser interface for remote administration and configuration of camera parameters. The browser interface shall provide PTZ control including preset and pattern and on-screen display (OSD) for access to camera programming.

F. The indoor/outdoor network positioning camera shall have a window blanking feature to conceal user-defined privacy areas that cannot be viewed by an operator. The indoor/outdoor camera dome system shall support up to eight blanked windows. A blanked area shall appear on the screen as a solid gray window.

G. The indoor/outdoor network positioning camera shall feature open architecture connectivity for third-party software recording solutions allowing integration into virtually any IP-based system. It is also compatible with Endura and Digital Sentry® video management systems. As with all Pelco IP camera solutions, Spectra® IV IP is Endura Enabled™ to record, manage, configure, and view multiple live streams.

H. The network camera shall provide an additional processor for running Pelco Video analytics.

I. Pelco Analytic Suites shall be configured and enabled using a standard Web browser.

J. Pelco Analytic Suites shall allow remote operation and alarm notification when used with an Endura system or a third-party system that supports Pelco's Analytics API.

K. Pelco Analytics for EP High Definition Digital Network Cameras including:

L. Abandoned Object: Detects objects placed in a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows. An airport terminal is a typical installation for this behavior. This behavior can also detect objects left behind at an ATM, signaling possible card skimming.

M. Adaptive Motion: Detects and tracks objects that enter a scene and then triggers an alarm when the objects enter a user-defined zone. This behavior is primarily used in outdoor environments with light traffic to reduce the number of false alarms caused by environmental changes.

N. Camera Sabotage: Detects contrast changes in the field of view. An alarm is triggered if the lens is obstructed with spray paint, a cloth, or a lens cap. Any unauthorized repositioning of the camera also triggers an alarm.

O. Directional Motion: Generates an alarm in a high traffic area when a person or object moves in a specified direction. Typical installations for this behavior include an airport gate or tunnel where cameras can detect objects moving in the opposite direction of the normal flow of traffic or an individual entering through an exit door.

P. Loitering Detection: Identifies when people or vehicles remain in a defined zone longer than the user-defined time allows. This behavior is effective in real-time notification of suspicious behavior around ATMs, stairwells, and school grounds.

Q. Object Counting: Counts the number of objects that enter a defined zone or cross a tripwire. This behavior might be used to count the number of people at a store entrance/exit or inside a store where the traffic is light. This behavior is based on tracking and does not count people in a crowded setting.

R. Object Removal: Triggers an alarm if an object is removed from a defined zone. This behavior is ideal for customers who want to detect the removal of high value objects, such as a painting from a wall or a statue from a pedestal.

S. Stopped Vehicle: Detects vehicles stopped near a sensitive area longer than the user-defined time allows. This behavior is ideal for airport curbside drop-offs, parking enforcement, suspicious parking, traffic lane breakdowns, and vehicles waiting at gates.

T. Pelco Analytic Suites shall be preloaded or configuration and alarm notification when used with an Endura® system or a third-party system that supports Pelco's Analytics API.

U. Multiple Pelco behaviors can be scheduled to work during a certain time or condition.

V. The indoor/outdoor fixed dome system shall meet or exceed the following design and performance specifications.

W. Camera Specifications

Sensor Type	1/3-inch, CCD
Optical Zoom	18X
Maximum Resolution	1280 x 960
Lens	f/1.6 (focal length, 4.7~84.6 mm optical)
Aspect Ratios	4:3 or 16:9
Light Sensitivity	f/1.6; 2,850ºK; SNR >24dB
Color (33 ms)	0.70 lux
Color (250 ms)	0.07 lux
Mono (33 ms)	0.25 lux
Mono (250 ms)	0.02 lux
Day/Night Capabilities	Yes
IR Cut Filter	Yes
IR Trace Curves	850 nm and 950 nm
Wide Dynamic Range	60dB
Iris Control	Auto iris with manual override
Backlight Compensation	Yes

Video Specifications

Compression	H.264 in High, Main, or Base profiles and MJPEG
Video Streams	Up to 2 simultaneous streams, the second stream variable based on the setup of the primary stream

Frame Rate - Up to 30, 25, 24, 15, 12.5, 12, 10, 8, 7.5, 6, 5, 4, 3, 2.5, 1 (depending upon coding, resolution, and stream configuration)

Available Resolutions

1.3 Megapixel	1280 x 1024; 5:4 aspect ratio; 20.0 ips max., 10.0 Mbps bit rate for MJPEG; 20.0 ips max., 3.4 Mbp4s bit rate for H.264
1.2 Megapixel	1280 x 960; 4:3 aspect ratio; 20.0 ips max., 9.8 Mbps bit rate for MJPEG; 20.0 ips max., 3.0 Mbps bit rate for H.264
0.9 Megapixel	1280 x 720; 16:9 aspect ratio; 30.0 ips max., 10.0 Mbps bit rate for MJPEG; 30.0 ips max., 2.9 Mbps bit rate for H.264
0.5 Megapixel	800 x 600; 4:3 aspect ratio; 30.0 ips max., 7.7 Mbps bit rate for MJPEG; 30.0 ips max., 2.0 Mbps bit rate for H.264
0.3 Megapixel	640 x 480; 4:3 aspect ratio; 30.0 ips max., 4.9 Mbps bit rate for MJPEG; 30.0 ips max., 1.5 Mbps bit rate for H.264

0.1 Megapixel 320 x 240; 4:3 aspect ratio; 30.0 ips max., 1.2 Mbps bit rate for MJPEG; 30.0 ips max., 0.5 Mbps bit rate for H.264

Additional 640 x 512, 640 x 352, 480 x 368, 480 x 272, 320 x 256, 320 x 176

Supported Protocols TCP/IP, UDP/IP (Unicast, Multicast IGMP),

UPnP, DNS, DHCP, RTP, RTSP, NTP, IPv4, SNMPv2c/v3, QoS, HTTP, HTTPS, LDAP (client), SSH, SSL, SMTP, FTP, and 802.1x (EAP)

Users

Unicast Up to 20 simultaneous users

Multicast Unlimited H.264

Security Access Password protected

Software Interface Web browser view and setup

Open IP Integration Pelco IP camera API

Minimum PC Requirements

Processor Intel Core® 2 Duo microprocessor, 2.6 GHz

Operating System Windows® XP, Windows Vista®, or
Mac OS® X 10.4 (or later)

Web User Interface Requires QuickTime® 7.55 (or later)

Memory 512 MB

Network Interface Card 100 Mbps

Monitor Minimum of 1024 x 768 resolution, 16- or 32-bit pixel color resolution

Web Browser Internet Explorer® 7.0 (or later); Mozilla®

Firefox® 3.5 (or later); Internet Explorer® 8.0 (or later) is recommended for configuring analytics

Media Player Pelco Media Player or QuickTime® 7.6.5 or

Microsoft Windows XP, Windows Vista, or QuickTime 7.6.4 for Mac OS X 10.4

Electrical Specifications

Ports RJ-45 for 100Base-TX; Auto MDI/MDI-X;

auto negotiate/manual setting

Cabling Type Cat5 cable or better for 100Base-TX

Input Voltage 18 to 32 VAC; 24 VAC nominal

22 to 27 VDC; 24 VDC nominal

Input Power

24 VAC 23 VA nominal (without heater);

73 VA nominal (with heater)

24 VDC 0.7 A nominal (without heater);

3 A nominal (with heater)

PoE IEEE802.3af (without heater)

Fuse 1.25 A

Dome Drive Specifications

Pan Speed - Variable between 400 per second continuous pan to 0.1º per second

Vertical Tilt - Unobstructed tilt of +0º to –90º

Manual Control Speed - Pan speed of 0.1º to 80º per second and pan at 150º per second in turbo mode; tilt operation shall range from 0.1º to 40º per second

Automatic Preset Speed Pan speed of 400º and a tilt speed of 160º per

second

Presets 255 positions with 16 preset tours

Preset Accuracy ± 0.1º

Proportional Pan/Tilt Speed Speed decreases in proportion to the increasing depth of zoom Motor Continuous duty and variable speed, operating at 18 to 32 VAC, 24 VAC nominal

Window Blanking 8, four-sided user-defined shapes, each side with different lengths; window blanking setting to turn off at user-defined zoom ratio; window blanking set to opaque gray or translucent smear; blank all video above user defined tilt angle; blank all video below user-defined tilt angle

Auto Flip Rotates dome 180º at bottom of tilt travel

Dome Drive Compatibility All dome drives are compatible with all back box

configurations

Power Consumption Nominal 23 VA (without heater running)Nominal 73 VA (with heater running)

Back box and lower dome specifications

Pendant, Environmental

Connection to Dome Drive Quick, positive mechanical and electrical

disconnect without the use of any tools

Installation Quick-mount wall, corner, pole, parapet, or ceiling adapter

Cable Entry Through 1.5-inch NPT fitting

Environmental Features Factory-installed heaters, blowers, and sun shroud

Operating Temperatures Maximum temperature range of –60°F to 140°F (–51°C to 60°C) for two hours and a continuous operating range of –22°F to 122°F (–30°C to 50°C)

Construction Aluminum

Trim Ring Connection 2 screws

Pendant, Standard

Connection to Dome Drive Quick, positive mechanical and electrical

disconnect without the use of any tools

Installation Quick-mount wall, corner, pole, parapet, or ceiling adapter

Cable Entry Through 1.5-inch NPT fitting

Environmental Features Factory-installed heaters, blowers, and sun shroud

Operating Temperatures Maximum temperature range of 113°F (45°C) for two hours and a continuous operating range of 25°F to 95°F (–4C° to 35°C)

Construction Aluminum

Trim Ring Connection 2 screws

In-Ceiling, Environmental

Connection to Dome Drive Quick, positive mechanical and electrical

disconnect without the use of any tools

Installation Hard Ceiling applications

Cable Entry 0.75-inch conduit fitting

Environmental Features Factory-installed heaters and blowers

Operating Temperatures maximum temperature range of –60°F to 140°F (–51°C to 60°C) for two hours and a continuous operating range of –22°F to 122°F (–30°C to 50°C)

Construction Aluminum

Trim Ring Connection 2 screws

Dome System Specifications

Diameter of Bubble, Maximum of 5.9 inches (15.0 cm)

Pendant, Environmental 10.6-inch (26.9 cm) overall length (including

dome) by 8.6-inch (21.8 cm) diameter

Pendant, Standard Pendant 10.6-inch (26.9 cm) overall length

(including dome) by 8.6-inch (21.8 cm) diameter

In-Ceiling, Environmental 4.4 inches (11.0 cm) above ceiling, lower dome

4.3 inches (10.9 cm) below ceiling, 8.6-inch (21.8 cm) diameter

In-Ceiling, Interior 5.2 inches (13.2 cm) above ceiling, lower dome 3.5 inches (8.8 cm) below ceiling, 8.2-inch (20.8 cm) diameter

Warranty

36-months, parts and labor

Certifications and Ratings

CE, Class A

FCC, Class A

UL/cUL Listed

C-Tick

Meets NEMA Type 4X and IP66 standards when installed properly

Pelco Model Numbers

The discreet camera dome system shall be the Pelco Spectra® HD

Exhibit B
City of Austin, Texas
EQUAL EMPLOYMENT/FAIR HOUSING OFFICE
NON-DISCRIMINATION CERTIFICATION

City of Austin, Texas
Human Rights Commission

To: City of Austin, Texas, ("OWNER")

I hereby certify that our firm conforms to the Code of the City of Austin, Section 5-4-2 as reiterated below:

Chapter 5-4. Discrimination in Employment by City Contractors.

Sec. 4-2 Discriminatory Employment Practices Prohibited. As an Equal Employment Opportunity (EEO) employer, the Contractor will conduct its personnel activities in accordance with established federal, state and local EEO laws and regulations and agrees:

(B) (1) Not to engage in any discriminatory employment practice defined in this chapter.

(2) To take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without discrimination being practiced against them as defined in this chapter. Such affirmative action shall include, but not be limited to: all aspects of employment, including hiring, placement, upgrading, transfer, demotion, recruitment, recruitment advertising; selection for training and apprenticeship, rates of pay or other form of compensation, and layoff or termination.

(3) To post in conspicuous places, available to employees and applicants for employment, notices to be provided by OWNER setting forth the provisions of this chapter.

(4) To state in all solicitations or advertisements for employees placed by or on behalf of the Contractor, that all qualified applicants will receive consideration for employment without regard to race, creed, color, religion, national origin, sexual orientation, gender identity, disability, veteran status, sex or age.

(5) To obtain a written statement from any labor union or labor organization furnishing labor or service to Contractors in which said union or organization has agreed not to engage in any discriminatory employment practices as defined in this chapter and to take affirmative action to implement policies and provisions of this chapter.

(6) To cooperate fully with OWNER's Human Rights Commission in connection with any investigation or conciliation effort of said Human Rights Commission to ensure that the purpose of the provisions against discriminatory employment practices are being carried out.

(7) To require compliance with provisions of this chapter by all subcontractors having fifteen or more employees who hold any subcontract providing for the expenditure of $2,000 or more in connection with any contract with OWNER subject to the terms of this chapter.

For the purposes of this Offer and any resulting Contract, Contractor adopts the provisions of the City's Minimum Standard Nondiscrimination Policy set forth below.

City of Austin
Minimum Standard Non-Discrimination in Employment Policy:

As an Equal Employment Opportunity (EEO) employer, the Contractor will conduct its personnel activities in accordance with established federal, state and local EEO laws and regulations.

The Contractor will not discriminate against any applicant or employee based on race, creed, color, national origin, sex, age, religion, veteran status, gender identity, disability, or sexual orientation. This policy covers all aspects of employment, including hiring, placement, upgrading, transfer, demotion, recruitment, recruitment *advertising, selection for training and apprenticeship, rates of pay or other forms of compensation, and layoff or termination.*

Further, employees who experience discrimination, sexual harassment, or another form of harassment should immediately report it to their supervisor. If this is not a suitable avenue for addressing their complaint, employees are advised to contact another member of management or their human resources representative. No employee shall be discriminated against, harassed, intimidated, nor suffer any reprisal as a result of reporting a violation of this policy. Furthermore, any employee, supervisor, or manager who becomes aware of any such discrimination or harassment should immediately report it to executive management or the human resources office to ensure that such conduct does not continue.

Contractor agrees that to the extent of any inconsistency, omission, or conflict with its current non-discrimination employment policy, the Contractor has expressly adopted the provisions of the City's Minimum Non-Discrimination Policy contained in Section 5-4-2 of the City Code and set forth above, as the Contractor's Non-Discrimination Policy or as an amendment to such Policy and such provisions are intended to not only supplement the Contractor's policy, but will also supersede the Contractor's policy to the extent of any conflict.

UPON CONTRACT AWARD, THE CONTRACTOR SHALL PROVIDE A COPY TO THE CITY OF THE CONTRACTOR'S NON-DISCRIMINATION POLICY ON COMPANY LETTERHEAD, WHICH CONFORMS IN FORM, SCOPE, AND CONTENT TO THE CITY'S MINIMUM NON-DISCRIMINATION POLICY, AS SET FORTH HEREIN, OR THIS NON-DISCRIMINATION POLICY, WHICH HAS BEEN ADOPTED BY THE CONTRACTOR FOR ALL PURPOSES (THE FORM OF WHICH HAS BEEN APPROVED BY THE CITY'S EQUAL EMPLOYMENT/FAIR HOUSING OFFICE), WILL BE CONSIDERED THE CONTRACTOR'S NON-DISCRIMINATION POLICY WITHOUT THE REQUIREMENT OF A SEPARATE SUBMITTAL.

Sanctions:
Our firm understands that non-compliance with Chapter 5-4 may result in sanctions, including termination of the contract and suspension or debarment from participation in future City contracts until deemed compliant with the requirements of Chapter 5-4.

Term:
The Contractor agrees that this Section 0800 Non-Discrimination Certificate or the Contractor's separate conforming policy, which the Contractor has executed and filed with the Owner, will remain in force and effect for one year from the date of filing. The Contractor further agrees that, in consideration of the receipt of continued Contract payments, the Contractor's Non-Discrimination Policy will automatically renew from year-to-year for the term of the underlying Contract.

Dated this 30th day of July, ______

CONTRACTOR Schneider Electric
Authorized Signature
Title John C Collis
VP South Region