Request for Proposal  
District Wide Security Access System

Pima County Community College District ("College" or "District") is seeking proposals from qualified firms to provide and install a District wide system for Proximity Card access and event recording of certain doors at assorted campuses.

A mandatory pre-proposal conference will be held on: **December 18, 2012 at 8:30 AM (Arizona Time)** at

Pima Community College  
Maintenance & Security  
6680 S. Country Club  
Tucson, AZ 85706  
MS 105

Immediately following the meeting there will be site visits. All attendees must have representation for these visits. You must call 520-206-4759 to reserve your spot on our vans (limit 2 people per vendor).

The deadline for receipt of sealed proposals is: **January 24, 2013 at 3:00 PM (Arizona Time)**. Sealed proposals must be received by this deadline at the following location:

Pima County Community College District  
District Finance Office-Purchasing  
4905D East Broadway, Room D-232  
Tucson, Arizona 85709-1420

Any proposal received after the date and time listed above will be returned and will not be considered.

Questions pertaining to this Request for Proposal (RFP) must be communicated in writing and be received via email by **January 3, 2013 at 3:00 PM (Arizona Time)**. Questions must be sent to the email address below and should include the specified Buyer’s name and proposal number, and any question(s) should include a reference to the appropriate page and section number of the RFP. Questions and answers will be posted on the Pima Community College webpage listed below by **January 10, 2013 at 5:00 PM (Arizona Time)**:

Jan Posz, C.P.M., Sr. Buyer  
DO-Staff-FO-Procur@pima.edu

Copies of the Request for Proposal, questions and answers, and any related documents are available on the Pima Community College Website:

http://www.pima.edu/administrative-services/purchasing/current-requests-for-proposals-bids-quotes.html

Purchasing Director  
Pima County Community College District  
District Finance Office-Purchasing  
4905 East Broadway, Room D-232  
Tucson, Arizona 85709-1420
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1</td>
<td>Project Summary</td>
</tr>
<tr>
<td>Section 2</td>
<td>Proposal Preparation and Submittal</td>
</tr>
<tr>
<td>Section 3</td>
<td>Selection and Contract Award</td>
</tr>
<tr>
<td>Section 4</td>
<td>Proposal Form</td>
</tr>
<tr>
<td>Section 5</td>
<td>Agreement</td>
</tr>
<tr>
<td>Section 6</td>
<td>Indemnification and Insurance Requirements</td>
</tr>
<tr>
<td>Section 7</td>
<td>Terms and Conditions</td>
</tr>
<tr>
<td>Attachment A</td>
<td>Forms:</td>
</tr>
<tr>
<td></td>
<td>Bidders Information</td>
</tr>
<tr>
<td></td>
<td>Federal Debarred Certification</td>
</tr>
<tr>
<td></td>
<td>Cost Proposal</td>
</tr>
<tr>
<td>Attachment B</td>
<td>Project Manual &amp; Construction Documents</td>
</tr>
</tbody>
</table>
Section 1
Project Summary

1. Request for Proposal Summary
Pima County Community College District ("College" or "District") is seeking proposals from qualified firms for the **District Wide Security Access System** in accordance with the Scope of Work specified in this Request for Proposal (RFP).

Pima Community College seeks to purchase and have installed, as a turn-key project, a District-wide system for Proximity Card access and event recording of certain doors at assorted campuses. The work includes the installation of the necessary hardware, software, licensing, and miscellaneous work, demolition, and repair.

2. Entity Submitting RFP. The terms “vendor”, “proposer”, “offerer”, “firm”, “consultant”, “company” or “contractor” used in this RFP or any subsequent documents or communications related to this RFP are interchangeable and mean the entity submitting a proposal and seeking to enter into a contract for the goods and/or services requested in this RFP.

3. Description of Pima County Community College District
Pima County Community College District, located in Tucson, Arizona, is one of the ten largest multi-campus, multi-site Community Colleges in the United States. The College is a two-year institution offering both occupational and traditional college courses, and awards many different degrees and certificates. The College’s comprehensive curriculum includes credit courses, workforce development programs (Center for Training and Development), adult education special programs (GED), as well as corporate and community based non-credit instruction. Students attend classes at six major campuses including the Community Campus, which itself holds classes at over 70 locations in Southern Arizona. The College employs more than 1,400 regular employees, approximately 1,500 adjunct faculty and 500 part-time personnel. More than 70,000 students attend credit and non-credit classes annually. The population for the Tucson metro area is over 1 million people. The College is accredited by the Commission on Institutions of Higher Education of the North Central Association of Colleges and Schools.
Section 2
Proposal Preparation and Submittal

Proposals must conform to all requirements stated below, and elsewhere in this RFP. Disregarding these requirements may result in disqualification of the proposal.

Before submitting a proposal, each firm shall familiarize itself with the entire RFP, including Scope of Work, contract form and all laws, regulations and other factors affecting contract performance. The firm shall be responsible for fully understanding the requirements of a subsequent contract and otherwise satisfy itself as to the expense and difficulties accompanying the fulfillment of contract requirements. The submission of a proposal will constitute a representation of compliance by the firm. There will be no subsequent financial adjustment for lack of such familiarization.

All proposal materials must be placed in a sealed package (envelope, box, etc.) clearly marked with the proposal name and number and the firm’s name. It is the responsibility of the firm to ensure that proposals are received in the Office of the Purchasing Director by the due date and time stated on page 1 of this RFP. The firm is responsible for delivery of their proposal by the deadline notwithstanding any claims of error or failure to perform by a mail, courier or package delivery service. No proposals or proposal modifications may be submitted orally, electronically, or via telephone, facsimile, electronic mail (email) or telegraph.

All proposals must be typewritten on standard paper size (8½ x 11 inches) and shall be in the required format incorporating the forms provided in this RFP package, if any. It is permissible to copy these forms as required. The authorized person signing the proposal shall initial erasures, interlineations or other modifications on the proposal.

The firm’s proposal should be organized in sections as outlined below:

1. **Cover Letter**
   All proposals must include a cover letter submitted under the firm’s name on the firm’s letterhead containing the signature and title of a person or an official of the firm who is authorized to commit the firm to a potential contract with the College. The cover letter must also identify the primary contact for this proposal and include the College’s RFP number found within this RFP. The cover letter should express the firm’s interest and serve as an executive summary of the proposal. Claims of proprietary information must be included in the cover letter.

2. **Proposal Form**
   All proposals must include the complete Proposal Form signed by a person or an official authorized to commit the firm to a contract with the District.

3. **Proposal Copies**
   The firm must submit one (1) original copy of the proposal, clearly marked “Original”. In addition, the firm must submit one (1) digital .PDF copy of the proposal on media suitable for copying and distributing electronically.
4. Qualifications
The proposal verbiage must describe the firm’s qualifications to provide the requested products and/or services, and include the following:
   a. Description of the nature of the firm’s business; include a description of experience, competencies, and overall organizational capabilities.
   b. Corporate organization chart indicating key management team members.
   c. Number of years in business.
   d. Description of the firm’s capabilities to provide the requested product(s)/service(s).
   e. Description of the project staff structure, the background, qualifications and relevant experience of all staff involved in the project, including length of time at contractor; include the responsibilities that each staff member will have during the execution of this project.
   f. Overview of approach and description of methodology to be used.
   g. Description of project structure and detailed project timelines and phases (if applicable).
   h. References: The proposer must provide three (3) independent references from three (3) different projects of similar scope, nature, and complexity to that requested by the College. The College prefers educational or governmental entity references. Each of the references must include the following information:
      i. Entity Name
      ii. Industry Type
      iii. Address, City, Province/State/Country
      iv. Contact Name, Title, Phone Number, and Email address
      v. Year(s) service(s) provided
      vi. Comments (include details regarding the current status of the product/service provided by proposer)

5. Response to Scope of Work
Responses must be clear and thorough, but concise, and written in plain, easy to understand language. Responses must follow the numbering format used in the Scope of Work section.

6. Exceptions Requested
Any exceptions to the requirements of this RFP that the firm requests the College to consider must be placed in this section. Each alternate or exception should be addressed separately with specific reference to the requirement. If there are no proposed alternates or exceptions, a statement to that effect must be included in this section of the proposal. Any proposed terms and conditions, contracts, waivers, licenses or agreements required by the firm should be included here with a brief explanatory introduction.

7. PROPRIETARY INFORMATION
In the event any proposer shall include in the proposal any information deemed "proprietary" or "protected," such information shall be separately packaged from the balance of the proposal and clearly marked as to any proprietary claim. The College discourages the submission of such information and undertakes to provide no more than reasonable efforts to protect the proprietary nature of such information. The College, as a public entity, cannot and does not warrant that proprietary information will not be disclosed. The College shall have the right to use any and all information included in the proposals submitted unless the information is expressly restricted by the proposer.
8. Cost Proposal
A detailed cost proposal must be provided and placed in a separate, sealed envelope, marked “Cost Proposal”, clearly marked with the proposal number and the firm’s name. If a Cost Proposal sheet is provided in this RFP, firms should complete it and use it as a guide to prepare their detailed cost proposal. One (1) copy of the Cost Proposal is required to be included with the original proposal. This information will not be considered during the initial stages of the evaluation process. Additional requirements are as follows:

a. Prices shall be shown by item and individually extended, unless otherwise indicated. In case of a conflict between unit price and extension, unit price prevails.

b. All applicable taxes are to be paid by the Proposer and included in the quoted price. The College is not exempt from paying State and local transaction privilege tax (sales tax).
   i. Proposals that include equipment or materials should not include sales tax in the amount of your proposal, but do show tax percentage in the appropriate space.
   ii. Proposals for services must include any applicable taxes as a separate itemized amount and also show tax percentage in the appropriate space.

c. Provide detailed explanations of any assumptions that the proposer made in calculating the project costs in order to provide sufficient information for the College to be able to prepare a detailed cost analysis and comparison.

Specify how proposer proposes that costs be billed to the College (e.g. actual expenses (time and materials), flat fee, capped, not-to-exceed, etc.) and

a. when the proposer proposes to bill the College for the expenses (e.g. progress payments, milestone, weekly, monthly, etc.)

b. Indicate if the proposal includes work in separate phases or sections. If so, provide separate sections identifying costs for each of the proposed phases and describe the proposed work that would be accomplished in each of the phases.

c. Indicate if any items are optional and specify them in a separate section(s).

d. State warranty information and maintenance costs after warranty period. Responses must include itemized maintenance of hardware and software support costs for up to five years.

9. Appendix
The Proposal Appendix must include:

a. All documents or forms required by the College to be completed by the firm including the required documents specified in the Appendix of this RFP.

b. Details of any litigation your company or any of its subsidiaries or affiliates has had in the past five years relate to the performance of services provided by your firm.

c. If a firm has had any previous contracts canceled or is currently debarred, suspended, or proposed for debarment by any government entity, the current status must be documented in this proposal. The firm agrees to notify the College of any change in this status. If any customer has stopped using the product(s) or service(s) you are proposing, provide details including customer name, date when product was installed, date when product was discontinued (usage) and reason for discontinuation, including contact details of the customer.

d. If the firm intends to use any cooperative, subcontract, third party agreement, or the like to perform under their proposal, the firm must supply the name, address, qualifications and criteria used by the firm for selection of any third party, and the intended services to be performed. The services provided under the scope of work proposed, in part or in whole, shall not be subcontracted our assigned without prior written permission of the College, except that the contractor may, without prior approval and without being released from any of its responsibilities hereunder, assign the contract to any affiliate or wholly-owned subsidiary of the contractor.

e. Samples of any documentation or form that proposer will require the College to sign.
10. General
   a. **Cost of Proposal Preparation** – The College shall not reimburse the cost of developing, presenting or providing any response to this solicitation; offers submitted for consideration should be prepared simply, and economically, providing adequate information in a straightforward and concise manner.

   b. **Certification** – By signature on the Proposal Form included herein, the consultant certifies that the submission of the proposal did not involve collusion or other anti-competitive practices. The consultant has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant in connection with the submitted proposal. In addition, consultant certifies whether or not an employee of the College has, or whose relative has, a substantial interest in any agreement subsequent to this document. Consultant also certifies their status with regard to debarment, or suspension by any governmental entity.

   Failure to provide a valid signature affirming the stipulations required by this clause shall result in the rejection of the submitted proposal and, if applicable, any resulting agreement. Signing the certification with a false statement shall void the proposal and, if applicable, any resulting agreement. Any resulting agreement may be subject to legal remedies provided by law. Consultant agrees to promote and offer to the College only those services and/or materials as stated in and allowed for under resulting agreement(s).
Section 3
Selection and Contract Award

Proposals shall be evaluated based on the requirements set forth in the RFP. Selection of the firm(s) will be at the discretion of the College and will be based on the proposal that the College deems to be the most responsive and responsible and serves the best interests of the College. It is the intent of the College to negotiate and enter into a contract with the selected firm following a Notice of Intent of Selection.

Selected proposer(s) may be required to make on-site oral and visual presentations or demonstrations at the request of the College. The College will schedule the time and location for any presentations. Costs and equipment for such presentations are the responsibility of the proposer. Best and Final offers may be solicited from the pool of finalists prior to selection of the successful firm.

Proposals will be reviewed by a selection committee and will be evaluated based on the following criteria listed in relative order of importance:

a. Firm Experience and Qualifications (to include information requested in Section 2, #4)
   i. Experience with projects of similar type and scope.
   ii. Experience with private and public sector organizations, and institutions of higher education.

b. Financial Viability
   i. Contractor’s ongoing financial viability to provide services to the College. Responses must include most recent audited financial statement.

c. Product design and capabilities (to include compliance with summary of work Section 01 11 00 Project Manual).

d. Project Methodology and Structure (if specified in Scope of Work).
   i. Description of the approach, methodology, and project structure to be used to satisfy the College’s project scope and objectives.

e. Cost Proposal
   i. Total cost to College as it relates to the services. Include warranty information and maintenance costs for up to 5 years.

f. Staff Expertise / Implementation and Operational Teams
   i. The experience of staff proposed to be involved in the project.
   ii. Proven and demonstrated hands-on expertise of key management team members and staff in this area of work.
   iii. Demonstrated expertise in being a strategic partner with clients.

g. References
   i. Feedback from submitted references.

h. Implementation and/or delivery schedule
   i. Proposed timeline reasonableness and responsiveness to project’s intended outcomes.
Section 4
Proposal Form

Date ________________________________

Proposal of ________________________________________,
(Name)
a corporation organized and existing under the laws of the State of ______________________; a partnership consisting of ________________________________________; an individual trading as _________________________________________________________________.
(Name)

Request for Proposal: ______________________________________
[provide title or brief description]

To:  Pima County Community College District (“College”)

1. In compliance with your Request for Proposal No. __________, the undersigned hereby offers to furnish the services designated in the RFP, in strict accordance with the RFP, upon written notice of acceptance of this Proposal at any time within thirty (30) days after the date of opening of the Proposals, and to execute the Contract in accordance with the Proposal as accepted within five (5) days after the Contract is presented for signature.

2. The undersigned Proposer hereby acknowledges receipt of the following Addenda, if any:

   Addendum No.          Date
   _______________________  _______________________  
   _______________________  _______________________  
   _______________________  _______________________  
   _______________________  _______________________  
   _______________________  _______________________  

3. The undersigned Proposer understands that the College reserves the right to reject any or all Proposals or to waive any formality or technicality, as determined by the College in its sole discretion, in any Proposal in the interest of the College.

4. The undersigned Proposer hereby certifies and affirms that this Proposal is genuine and not a sham or collusive, nor made in the interest or behalf of any person not herein named, and that the undersigned Proposer has not directly or indirectly induced or solicited any other Proposer to put in a sham bid, or any other person, firm, or corporation to refrain from bidding, and that the Proposer has not in any manner sought by collusion to secure for itself an advantage over any other Proposer.

5. The undersigned certifies that to the best of his/her knowledge: (check only one)
( ) There is no officer or employee of Pima Community College who has, or would have, or whose relative has, or would have, a substantial interest in any contract resulting from this request.

( ) The names of any and all public officers or employees of Pima Community College who have, or would have, or whose relative has, or would have, a substantial interest in any contract resulting from this request, and the nature of the substantial interest, are included below or as an attachment to this Proposal.

6. The Proposer certifies, to the best of its knowledge and belief, that:

(i) The Proposer and/or any of its Principals or Owners:

(A) (check one) are ( ) or are not ( ) presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any governmental agency.

(B) (check one) have ( ) or have not ( ), within a three year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain or performing a public (federal, state or local) contract or subcontract; violation of federal or state antitrust statutes, rules or regulations relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion; or receiving stolen property; and

(C) (check one) are ( ) or are not ( ) presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any other of the offenses enumerated in paragraph (i)(B) of this provision.

(ii) The Proposer (check one) has ( ) or has not ( ), within a three year period preceding this offer, had one or more contracts terminated for default by any governmental agency.

"Principals," for the purposes of this Proposal, means officers, directors, owners, partners and persons having primary or substantial management or supervisory responsibilities within a business entity.
7. The certifications in paragraphs 4, 5 and 6 of this Proposal are material representations of fact upon which reliance will be placed when making an award. If it is later determined that the Proposer knowingly rendered an erroneous certification, in addition to other remedies available to the College, the College may terminate the contract resulting from this solicitation for default.

____________________________________
(Official Name of Firm)

____________________________________
(Signature)

____________________________________
(Print Name)

____________________________________
(Title)

____________________________________
(Complete Business Address)

____________________________________
(Email Address)

____________________________________
(Federal Taxpayer ID Number)
Section 5
AGREEMENT

AGREEMENT BETWEEN PIMA COUNTY COMMUNITY COLLEGE DISTRICT

AND

(insert vendor name)

This Agreement made and entered into on the _____ day of __________, 20_, by and between Pima County Community College District hereinafter referred to as “District” or “College” and ________________ hereafter referred to as the “Vendor.”

Drawings and Specifications for this Project were prepared by ________________________________ (Owner’s Representative, hereinafter referred to as ‘OR’), who shall act as OR pursuant to the Contract Documents.

The District and the Vendor agree as follows:

FIRST: The Vendor agrees to perform the professional, technical and/or management services hereinafter set forth when, and as assigned by the District, and

SECOND: The District agrees to pay the Vendor a fee, together with such other payments and reimbursements as are hereinafter provided.

ARTICLE 1: VENDOR’S SERVICES
The Vendor agrees to provide services to the District as outlined in the Project Manual & Construction Documents in Attachment B of this Agreement which is hereby referenced and incorporated as an integral part of this Agreement. All work performed under the Agreement must have prior approval of the District.

ARTICLE 2: PAYMENT STRUCTURE
The payment structure for the work conducted under this Agreement will be in accordance with Vendors Cost Proposal which is hereby referenced and incorporated as an integral part of this Agreement.

ARTICLE 3: METHOD OF PAYMENT
Payments to the Vendor will be made upon the presentation and approval of the Vendor’s invoice. Each such invoice shall be documented in such detail and demonstrate such progress on each portion of the work as the District may reasonably require.

ARTICLE 4: INDEMNIFICATION
To the fullest extent permitted by law, the Vendor shall defend, indemnify and hold harmless the District, its agents, representatives, officers, directors, officials and employees, from and against all claims, damages, losses and expenses (including, but not limited to, attorneys’ fees, court costs and the cost of appellate proceedings) relating to, arising out of, or alleged to have resulted from the acts, errors, mistakes, omissions, work or services of the Vendor, its employees, agents or any tier of subcontractors
in the performance of the Agreement. Vendor’s duty to defend, hold harmless and indemnify the District, its agents, representatives, officers, directors, officials and employees, shall arise in connection with any claim, damage, loss or expense that is attributable to bodily injury, sickness, disease, death or injury to, impairment or destruction of property, including loss of use resulting therefrom, caused by any acts, errors, mistakes, omissions, work or services in the performance of the Agreement, including any employee of the Vendor or any tier of subcontractor or any other person for whose acts, errors, mistakes, omissions, work or services the Vendor be legally liable.

ARTICLE 5: EMPLOYEE RELATIONSHIP
The Vendor is an independent contractor and is not an employee, partner, legal representative, joint venturer or agent of the District. The District is not an employee, partner, legal representative, joint venturer or agent of the Vendor.

ARTICLE 6: CANCELLATION
This Agreement may be cancelled at any time, with or without cause, by the District giving seven (7) days written notice to the Vendor. In the event of such cancellation, the Vendor shall be paid for authorized services provided prior to the effective date of termination. In ascertaining the services actually rendered hereunder up to the date of the termination of this Agreement, consideration shall be given to both completed work and work in process of completion and to complete and incomplete reports and other documents whether delivered to the District or in the possession of the Vendor.

ARTICLE 7: OWNERSHIP OF DRAWINGS OR REPORTS
Services as represented on drawings, reports, memoranda, notes and drafts are the property of the District whether the work is completed or not and may be used by them in any fashion they see fit. Notwithstanding the foregoing, however, the Vendor reserves the right to use any studies, analyses or data prepared or collected during the course of this work for other purposes as seen fit, provided, however, that no such use shall allow the District to be identified without the consent of the District.

ARTICLE 8: PERSONAL SERVICES
It is agreed that the District is relying on the personal services of the Vendor and upon their technical ability and professional integrity. Such reliance is one of the chief considerations for the execution of this Agreement by the District. It is further understood and agreed that the Vendor shall not assign, sublet nor transfer his duties under this Agreement, nor shall this Agreement be assignable or transferable by operation of law or otherwise without the written consent of the District.

ARTICLE 9: CONFLICT OF INTEREST
The Vendor agrees to perform services exclusively for the District under this agreement, and expressly agrees not to undertake any conflicting duties to others, with or without compensation, which could in any way compromise that responsibility. The Vendor shall not disclose to others any confidential information gained from this relationship without the prior, written permission from the District, and the Vendor shall not seek to use their position, the information gained thereby, nor any other aspect of the project or relationship with others involved in it, for personal gain or other remuneration or benefit, beyond the compensation provided for herein.

ARTICLE 10: GOVERNING LAW
This Agreement is made in the State of Arizona and shall be subject to and governed by the laws of the State of Arizona. All questions concerning the validity, construction and administration of the Agreement shall be determined under Arizona law.
ARTICLE 11: SEVERABILITY
This Agreement shall be severable and to the extent that any part of the Agreement is unenforceable for any reason whatsoever, the remaining parts of this Agreement shall remain in full force and effect.

ARTICLE 12: NOTICES
All notices to either party shall be deemed to have been provided by depositing the same, postage pre-paid, with the United States Postal Service, addressed as follows:

District Representative:

Vendor Representative:

ARTICLE 13: ARBITRATION
If the parties are unable to resolve any disputes arising under the Agreement, those disputes shall be resolved through arbitration in accordance with A.R.S. ' 12-1501, et. seq.

ARTICLE 14: NON-DISCRIMINATION
The parties agree to comply with Arizona law prohibiting discrimination in employment by government contractors, to the extent applicable with this Agreement, along with other applicable non-discrimination laws and regulations.

ARTICLE 15: LACK OF SUFFICIENT FUNDING
This Agreement may be cancelled without any further obligation on the part of the College in the event that sufficient appropriated funding is unavailable to assure full performance of the Agreement terms. Vendor shall be notified in writing of any such non-appropriation at the earliest opportunity.

ARTICLE 16: INSURANCE
Vendor shall furnish insurance as required by Section 6 hereto, which is incorporated herein by this reference as though fully set forth herein.

ARTICLE 17: ADDITIONAL TERMS AND CONDITIONS
The parties shall comply with the Terms and Conditions attached hereto as Section 7, which are incorporated herein by this reference as though fully set forth herein.

IN WITNESS WHEREOF, the Parties to this agreement have hereunto caused the same to be executed at Tucson, Arizona the day and year first above written.

Pima County Community College District: Vendor:

By: ____________________________ By: ____________________________

Title: __________________________ Title: __________________________
Section 6
Indemnification and Insurance Requirements

1. Indemnification
To the fullest extent permitted by law, the contractor shall defend, indemnify and hold harmless the College, its agents, representatives, officers, directors, officials and employees from and against all claims, damages, losses and expenses (including but not limited to attorney fees, court costs, and the cost of appellate proceedings), relating to, arising out of, or alleged to have resulted from the acts, errors, mistakes, omissions, work or services of the contractor, its employees, agents, or any tier of subcontractors in the performance of the contract. The contractor’s duty to defend, hold harmless and indemnify the College, its agents, representatives, officers, directors, officials and employees shall arise in connection with any claim, damage, loss or expense that is attributable to bodily injury, sickness, disease, death, or injury to, impairment, or destruction of property including loss of use resulting there from, caused by any acts, errors, mistakes, omissions, work or services in the performance of this contract including any employee of the contractor or any tier of subcontractor or any other person for whose acts, errors, mistakes, omissions, work or services the contractor be legally liable. The amount and type of insurance coverage requirements set forth herein will in no way be construed as limiting the scope of the indemnity in this paragraph.

The contractor shall hold the District, its officers and employees, harmless from liability of any nature or kind on account of use of any copyrighted or non-copyrighted composition, secret process, patented or unpatented invention, article or appliance furnished or used under this request.

2. Insurance Requirements
The contractor, at contractor’s own expense, shall purchase and maintain the herein stipulated minimum insurance with companies duly licensed to do business in the State of Arizona with policies and forms satisfactory to the College and possessing a minimum current A.M. Best, Inc. Rating of B++6.

All insurance required herein shall be maintained in full force and effect until all work required to be performed under the terms of the Contract is satisfactorily completed and formally accepted; failure to do so may, at the sole direction of the College, constitute a material breach of this Contract.

The contractor’s insurance shall be primary insurance, and any insurance or self-insurance maintained by the College shall not contribute to it.

Any failure to comply with the claim reporting provisions of the policies or any breach of an insurance policy warranty shall not affect coverage afforded under the policy to protect the College.

All policies, except Workers’ Compensation, shall contain a waiver of transfer rights of recovery (subrogation) against the College, its agents, representatives, directors, officers, and employees for any claims arising out of the contractor’s work or service.

The insurance policies may provide coverage which contains deductibles or self-insured retentions. Such deductible and/or self-insured retentions shall not be applicable with respect to the coverage provided to the College under such policies. The contractor shall be solely responsible for deductible and/or self-insured retention and the College, at its option, may require the contractor to secure the
payment of such deductible or self-insured retentions by a surety bond or an irrevocable and unconditional letter of credit.

The College reserves the right to request and to receive, within 10 working days, certified copies of any or all of the herein required insurance policies and/or endorsements. The College shall not be obligated, however, to review same or to advise the contractor of any deficiencies in such policies and endorsements, and such receipt shall not relieve the contractor from, or be deemed a waiver of the College’s right to insist on, strict fulfillment of contractor’s obligations under this Contract.

The insurance policies, except Workers’ Compensation, required by this Contract shall name the College, its agents, representatives, officers, directors, officials, and employees as Additional Insured.

3. Required Coverage:

   a. General Liability
      The contractor shall maintain and cause any subcontractor to maintain Commercial General Liability insurance with a limit of not less than $2,000,000 for each occurrence with a $2,000,000 Products and Completed Operations Aggregate and $2,000,000 General Aggregate Limit. The policies shall include coverage for bodily injury, broad form property damage, personal injury, products/completed operations and blanket contractual coverage including, but not limited to, the liability assumed under the indemnification provisions of this Contract, which coverage will be at least as broad as Insurance Service Office, Inc. Policy Form CG 000211093 or any replacement thereof. The coverage shall not exclude X, C, U.

      Such policies shall contain a severability of interest provision, and shall not contain a sunset provision or commutation clause, or any provision that would serve to limit third party action over claims.

      The Commercial General Liability additional insured endorsement shall be at least as broad as the Insurance Service Office, Inc.’s, Additional Insured, Form B, CG20101185, and shall include coverage for the contractor’s operations and products and completed operations.

   b. Workers’ Compensation
      The contractor shall carry Workers’ Compensation insurance to cover obligations imposed by federal and state statutes having jurisdiction of the contractor’s employees engaged in the performance of the work; and, Employer’s Liability insurance of not less than $2,000,000 for each accident, $1,000,000 disease for each employee, and $1,000,000 disease policy limit.

      In case any work is subcontracted, the contractor will require the Subcontractor to provide Workers’ Compensation and Employer’s Liability to at least the same extent as required of the contractor.

   c. Certificates of Insurance
      Prior to commencing Services under this contract, contractor shall furnish the College with Certificates of Insurance, or formal endorsements as required by the Contract, issued by contractor’s insurer(s), as evidence that policies providing the required coverages, conditions and limits required by this Contract are in full force and effect.
In the event any insurance policy(ies) required by this contract is(are) written on a “claims made” basis, coverage shall extend for two years past completion and acceptance of the contractor’s work or services and as evidenced by annual Certificates of Insurance.

If a policy does expire during the life of the contract, a renewal certificate must be sent to the College thirty (30) days prior to the expiration date.

All Certificates of Insurance required by this Contract shall be identified with a bid or proposal serial number and title.

d. Cancellation and Expiration Notice

Insurance evidenced by these certificates shall not expire, be canceled, or materially changed without thirty (30) days prior written notice to the College.
Section 7  
Terms and Conditions

1. Legal Remedies – All claims and controversies shall be subject to the Pima County Community College Policy regarding Formal Protests and Appeals

2. Agreement – The Agreement shall contain the entire agreement between the College and the Consultant relating to this requirement and shall prevail over any and all previous agreements, contracts, proposals, negotiations, purchase orders or master agreement in any form.

3. Agreement Amendments – The Agreement shall be modified only by a written amendment signed by persons duly authorized to enter into agreements on behalf of the College and the Consultant.

4. Provisions Required by Law – Each and every provision of law and any clause required by law to be in the Agreement shall be read and enforced as though it were included herein, and if through mistake or otherwise any such provision is not inserted, or is not correctly inserted, then upon the application of either party the Agreement shall forthwith be physically amended to make such insertion or correction.

5. Severability – The provisions of the Agreement are severable to the extent that any provision or application held to be invalid shall not affect any other provision or application of the Agreement which may remain in effect without the invalid provision or application.

6. Records – Pursuant to provisions of title 35, chapter 1, article 6 A.R.S. §35-215 the Consultant shall retain, and shall contractually require each subcontractor to retain, all books, accounts, reports, files and other records relating to the acquisition and performance of the Agreement for a period of five (5) years after the completion of the Agreement. All such documents shall be subject to inspection and audit at reasonable times. Upon request, a legible copy of any or all such documents shall be produced at the offices of the Auditor General, the Attorney General or the College Purchasing Office.

7. Advertising – Contractor shall not advertise or publish information concerning the Agreement, without prior written consent of the College.

8. Preparation of Specifications by Persons Other than College Personnel – All specifications shall seek to promote overall economy for the purposes intended and encourage competition and not be unduly restrictive in satisfying the College's needs. No person preparing specifications shall receive any direct or indirect benefit from the utilization of specifications, other than fees paid for the preparation of specifications.

9. Americans With Disabilities Act – The Consultant shall comply with all applicable provisions of the Americans With Disabilities Act and applicable federal regulations under the act.

10. Conflict of Interest – The College may, within three years after its execution, cancel the agreement without penalty or further obligation if any person significantly involved in negotiating, drafting, securing or obtaining the agreement for or on behalf of the College becomes an
employee of or a consultant in any capacity to any other party to the agreement with reference to
the subject matter of the Agreement while the Agreement or any extension thereof is in effect or
as otherwise provided by A.R.S. § 38-511..

11. Drug Free Workplace – The Consultant agrees that in the performance of the Agreement,
neither the Consultant nor any employee of the Consultant shall engage in the unlawful
manufacture, distribution, dispensing, possession, or use of a controlled substance in conducting
any activity covered in the Agreement. The College reserves the right to request a copy of the
Consultant Drug Free Workplace Policy. The Consultant further agrees to insert a provision
similar to this statement in all subcontracts for services required.

12. Equal Opportunity – The provisions of Section 202 of Executive Order 11246.41 C.F.R. Sec. -0-
1.4.41 Sec. 60-250.4 and 41 C.F.R. Sec. 60-741.4 are incorporated herein by reference and shall
be applicable to the Agreement unless the Agreement is exempted under the rules, regulations or
orders of the U.S. Secretary of Labor.

13. Federal, State and Local Taxes, Licenses and Permits – Consultant is solely responsible for
complying with all laws, ordinances, and regulations on taxes, registrations, licenses and permits,
as they may apply to any matter under this document. The Consultant must demonstrate that
they are duly licensed by whatever regulatory body may so require during the performance of the
Agreement. Prior to the commencement of Agreement, the Consultant shall be prepared to
provide evidence of such licensing as may be requested by the College. Consultant shall, at no
expense to the College, procure and keep in force during the entire period of the Agreement all
such permits and licenses.

14. Gratuities – The College may, by written notice to the Consultant, cancel the agreement if it is
found by the College that gratuities, in the form of entertainment, gifts or otherwise were offered
or given by the Consultant or any agent or representative of the contractor, to any officer or
employee of the College with a view toward securing an agreement or securing favorable
treatment with respect to the performing of such agreement.

15. Liens – Each Consultant shall keep the College free and clear from all liens asserted by any
person or entity for any reason arising out of the furnishing of services or materials by or to the
Consultant.

16. Sales and Use Tax – The College is not exempt from state sales and use tax.

17. Sexual Harassment – Federal law and the policies of the College prohibit sexual harassment of
College employees or students. Sexual harassment includes any unwelcome sexual advance
toward a College employee or student, any request to a sexual favor from a College employee or
student, or any other verbal or physical conduct of a sexual nature that is so pervasive as to
create a hostile or offensive working environment for College students. Consultant,
subcontractors and suppliers for this project are required to exercise control over their employees
so as to prohibit acts of sexual harassment of College employees and students. The employer of
any person whom the College, in its reasonable judgment, determines has committed an act of
sexual harassment agrees as a term and condition of the Agreement to cause such person to be
removed from the project site and from College premises and to take such other action as may be
reasonably necessary to cause the sexual harassment to cease.
18. Smoking – All facilities of the College are smoke free. Smoking is not permitted inside College buildings or within 25 feet of doorways and air intakes. The Consultant is required to comply with this smoke free policy.

19. Confidentiality – The parties shall comply with 20 USC Section 1232(g), the Buckley Amendment to the Family Educational Right and Privacy Act of 1974. Therefore, Contractor shall not be entitled to receive Employee or Student information directly from the College, other than public information available in any College directory which is not protected by federal or state privacy or confidentiality statutes or regulations. Contractor may solicit Employee and Student information directly from Employees and Students subject to prior disclosures by Contractor of all intended uses of such information. Regardless of the Employee or Student personal information, even if such information is publicly available via directories, Contractor shall under no circumstances sell, duplicate, market, or give to any person or persons, entities or other companies a list or other personal information of any or all Employees or Students. All Employee and Student identities and personal information shall remain confidential. Disclosure by Contractor occurring without the express prior written consent of the Employee or Student shall result in the immediate termination of this agreement.

20. Assignment-Delegation – No right or interest in the Agreement shall be assigned or delegated by Consultant without the prior written permission of the College. Any attempted assignment or delegation by Consultant shall be wholly void and totally ineffective for all purposes unless made in conformity with this paragraph.

21. Force Majeure – Neither party shall be liable in damages of have the right to terminate this Agreement for any delay or default in performing under the Agreement if such delay or default is caused by conditions beyond its reasonable control including, but not limited to wars, insurrections, fires, floods, governmental restrictions and/or any other cause beyond the reasonable control of the party whose performance is affected.

22. Intellectual Property Rights – It is understood and agreed that ownership of intellectual property developed as a result of fulfilling the requirements of this Agreement belongs solely and exclusively to the College. Documents provided in connection with the Agreement belong to the College and are being used with permission. Intellectual property, as used herein, means all forms of legally protectable intellectual property, including copyrights, trademarks, inventions, patent applications, patents and mask works, drawings and/or blueprints. It is also understood and agreed that any intellectual property created as a result of Consultant’s performance of this Agreement is considered a work for hire under the U.S. copyright laws and as such, the College will own the copyright.

23. Laws and Regulations – Consultants are solely responsible for keeping themselves fully informed of and faithfully observing all laws, ordinances, and regulations affecting the rights of their employees, and shall protect and indemnify the College, its officers and agents against any claims of liability arising from or based on any violation thereof.

24. Payment Terms – Payments by the College shall be subject to the provision of Title 35 of Arizona Revised Statutes, relating to time and manner of submission of claims. The College’s obligation is payable only and solely from funds appropriated for the purpose of the Agreement. Unless otherwise stated herein, the payment terms for the Agreement are Net 30 days.
25. **Price Adjustment** – Price changes will normally only be considered at the end of one Agreement period and the beginning of another. Price change requests shall be in writing, submitted at least sixty (60) days prior to the end of the current Agreement period, and shall be supported by written evidence of increased costs to the Consultant. The College will not approve unsupported price increases that will merely increase the gross profitability of Consultant at the expense of the College. Price change requests shall be a factor in the Agreement extension review process. The College shall, in its sole opinion, determine whether the requested price increase or an alternate option is in the best interest of the College.

26. **Prior Course of Dealings** – No trade usage, prior course of dealing, or course of performance under other agreements shall be a part of this Agreement resulting from this RFP, nor shall such trade usage, prior course of dealing or course of performance be used in the interpretation or construction of such resulting agreement.

27. **Right to Offset** – The College shall be entitled to offset against any sums due the Consultant, any expenses or costs incurred by the College, or damages assessed by the College concerning the Consultant’s non-conforming performance or failure to perform the Agreement, or any other debt owing the College.

28. **Insolvency** – The College shall have the right to terminate the Agreement at any time in the event Consultant files a petition in bankruptcy; or is adjudicated bankrupt; or if a petition in bankruptcy is filed against Consultant and not discharged within thirty (30) days; or if Consultant becomes insolvent or makes an assignment for the benefit of its creditors or an arrangement pursuant to any bankruptcy law; or if a receiver is appointed for Consultant or its business.

29. **Lack of Funding** – The Agreement may be canceled without further obligation on the part of the College in the event that sufficient appropriated funding is unavailable to assure full performance of the terms. The Consultant shall be notified in writing of such non-appropriation as soon as reasonably possible. No penalty shall accrue to the College in the event this cancellation provision is exercised. This cancellation provision shall not be construed so as to permit the College to terminate the Agreement in order to acquire similar equipment, material, supplies or services from another party.

30. **Stop Work Order** – The College may at any time, by written order to the Consultant, require the Consultant to stop all or any part of the work called for by the Agreement for a period of up to ninety (90) days after the order is delivered to the Consultant, and for any further period to which the parties may agree. The order shall be specifically identified as the Stop Work Order issued under this provision. Upon receipt of the order, the Consultant shall immediately comply with its terms and take all reasonable steps to minimize the incidence of costs allocable to the work covered by the order during the period of work stoppage. If a Stop Work Order issued under this provision is canceled or the period of the order or any extension expires, the Consultant shall resume work. The College shall make an equitable adjustment in the delivery schedule or Agreement price, or both, and the Agreement shall be amended in writing accordingly.

31. **Suspension or Debarment** – The College may by written notice to the Consultant immediately terminate the Agreement if the College determines that the Consultant has been debarred, suspended, or otherwise lawfully prohibited from participating in any public procurement activity, including but not limited to, being disapproved as a subcontractor or Contractor of any public procurement unit or other governmental body.
32. **Continuation of Performance Through Termination** – The Consultant shall continue to perform, in accordance with the requirements of Agreement, up to the date of termination, as directed in the termination notice.

33. **Sudan, or Iran Scrutinized Business** – Pursuant to A.R.S. #35-391.06(A) AND 35-393.06(B), Contractor certifies that it does not have a “scrutinized” business operation in either Sudan or Iran, as that term is defined in A.R.S. #35-391(15) AND 35-393(12) respectively.

34. **Federal Immigration Laws and Regulations** – Consultant warrants that it complies with all Federal Immigration laws and regulations that relate to its employees and complies with A.R.S. § 23-214(a) and that it requires the same compliance of all subcontractors under the agreement. Consultant acknowledges that pursuant to A.R.S. § 41-4401 and effective September 30, 2008, a breach of this warranty is a material breach of the agreement subject to penalties up to and including termination of the agreement. The College retains the legal right to audit the records of the Consultant and inspect the papers of any employee who works for the Consultant to ensure compliance with this warranty and the Consultant shall assist in any such audit. The Consultant shall include the requirements of this paragraph in each contract with subcontractors under the agreement.

If the Consultant or subcontractor warrants that it has complied with the employment verification provisions prescribed by sections 274(a) and 274(b) of the Federal Immigration and Nationality Act and the E-verify requirements prescribed by A.R.S. § 23-214(A), The Consultant or subcontractor shall be deemed to be in compliance with this provision. The College may request proof of such compliance at any time during the term of the Agreement by the Consultant and any subcontractor.

35. **Extended Contract**

   The College is an active member of the Strategic Alliance for Volume Expenditures (S.A.V.E.) Cooperative agreement. Under this Cooperative Purchasing Agreement, and with the concurrence of the successful Proposer, other members of this organization may access any subsequent agreement/contract resulting from this solicitation. If the Proposer does not want to grant such access, it must be stated in their Proposal. In the absence of a statement to the contrary, the college will assume that access is granted by the Proposer to any subsequent agreement/contract.
Attachment A

Forms

- Bidders Information
- Federal Debarred Certification
- Cost Proposal
BIDDER’S INFORMATION

Bidder shall state if this Proposal is submitted by an Individual, Partnership, or Corporation.

1. IF PARTNERSHIP, list names of all partners:

________________________________________________________________________

________________________________________________________________________

2. IF CORPORATION, give name of State in which corporation is registered:

________________________________________________________________________

Provide the names of the following Corporation officers:

President _______________________________________________________________________

Secretary _______________________________________________________________________

Treasurer _______________________________________________________________________

3. IF LICENSED CONTRACTOR, provide all contractor’s license number(s) applicable to this Proposal

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

4. Provide name of bonding company: ___________________________________________

    Total bonding capacity: $________________________________________

5. Name of Firm _____________________________________________________________

6. Telephone: ______________________ Fax: _________________________________
FEDERAL DEBARRED LIST CERTIFICATION

Certification Regarding Debarment, Suspension, Proposed Debarment, and Other Responsibility Matters (Dec 2001)

_________________
(Date)

District Finance Office – Purchasing
Pima Community College
4905 E Broadway Blvd.
Tucson, AZ 85709

In accordance with the Federal Acquisition Regulation, 52-209-5:

(a) (1) The Offeror certifies, to the best of its knowledge and belief, that-
   (i)  The Offeror and/or any of its Principals-
       (A) (check one) Are ( ) or are not ( ) presently debarred, suspended, proposed for
           debarment, or declared ineligible for the award of contracts by any Federal agency;
           (The debarred list (List of Parties Excluded from Federal Procurement and
           Nonprocurement Programs is at http://epls.arnet.gov on the Web)
       (B) (check one) Have ( ) or have not ( ), within a three-year period preceding this offer,
           been convicted of or had a civil judgment rendered against them for; commission of
           fraud or a criminal offense in connection with obtaining, attempting to obtain, or
           performing a public (Federal, state, or local) contract or subcontract, violation of
           Federal or state antitrust statutes relating to the submission of offers; or commission of
           embezzlement, theft, forgery, bribery, falsification or destruction of records, making
           false statements, tax evasion; or receiving stolen property; and
       (C) (check one) Are ( ) or are not ( ) presently indicted for, or otherwise criminally or
           civilly charged by a governmental entity with, commission of any of the offenses
           enumerated in paragraph (a) (1) (i) (B) of this provision.
   (ii)  The offeror (check one) has ( ) or has not ( ), within a three-year period preceding this
           offer, had one or more contracts terminated for default by any Federal agency.

   (2) “Principals”, for the purposes of this certification, means officers; directors’ owners’ partners’
   and, persons having primary management or supervisory responsibilities within a business
   entity (e.g. general manager, plant manager, head of a subsidiary, division, or business
   segment, and similar positions).

This Certification Concerns a Matter Within the Jurisdiction of an Agency of the United States and the
Making of a False, Fictitious, or Fraudulent Certification May Render the Maker Subject to Prosecution
Under Section 1001, Title 18, United States Code.

(a) The Offeror shall provide immediate written notice to the Contracting Officer, if, at any time prior
   to contract award, the Offeror learns that its certification was erroneous when submitted or has
   become erroneous by reason of changed circumstances.

(b) A certification that any of the items in paragraph (a) of this provision exists will not necessarily
   result in withholding of an award under this solicitation. However, the certification will be
   considered in connection with a determination of the Offeror’s responsibility. Failure of the
Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(c) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(d) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

(Firm) ____________________________________________
(email address) __________________________ (Phone) __________________________
(Signature) __________________________ (Fax) __________________________
(Print Name) __________________________ (Federal Taxpayer ID Number) __________________________
(Print Title) __________________________
Cost Proposal

District Wide Security Access System

Request for Proposal P13/9794

System, to include Installation  $__________________

Warranty  _________________ yr(s)

Maintenance Cost  $___________________ Year 1

Maintenance Cost  $___________________ Year 2

Maintenance Cost  $___________________ Year 3

Maintenance Cost  $___________________ Year 4

Maintenance Cost  $___________________ Year 5

Responses must include what is covered in the ongoing maintenance cost.
Attachment B
Project Manual & Construction Documents
PROJECT MANUAL
SECURITY AND ACCESS IMPLEMENTATION
for
PIMA COMMUNITY COLLEGE
Tucson, Arizona

NTD Architecture Project 2009-0118-01
April, 2012

ARCHITECT
NTD ARCHITECTURE
2940 N. SWAN AVE., SUITE 214
TUCSON, AZ 85712

2940 North Swan Road, Suite 214, Tucson, AZ 85712 (520) 784-0975
PROJECT MANUAL

for the Construction
of
Security and Access Implementation

for

Pima Community College

Prepared By

NTD Architecture
2940 North Swan Road, Suite 214
Tucson, AZ 85712

NTD # 2009-0118-01

April, 2012
# TABLE OF CONTENTS

## GENERAL DOCUMENTS
- Cover
- Flyleaf
- Table of Contents
- Directory

## DIVISION 00 – PROCUREMENT AND CONTRACTING REQUIREMENTS

- PCC to provide this list
- Notice Inviting Sealed Bids
- Instructions to Bidders
- Proposal
- List Of Subcontractors
- Bid Bond
- Payment Bond Pursuant
- Performance Bond Pursuant
- Notice of Award, Notice to Proceed and Receipt of Notice
- Contract and General Conditions Between Owner and Contractor

## DIVISION 01 – GENERAL REQUIREMENTS

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 11 00</td>
<td>Summary of Work</td>
</tr>
<tr>
<td>01 22 00</td>
<td>Unit Prices</td>
</tr>
<tr>
<td>01 26 00</td>
<td>Contract Procedures</td>
</tr>
<tr>
<td></td>
<td>RFI Form</td>
</tr>
<tr>
<td>01 33 00</td>
<td>Submittal Procedures</td>
</tr>
<tr>
<td>01 50 00</td>
<td>Temporary Facilities and Controls</td>
</tr>
<tr>
<td>01 73 29</td>
<td>Cutting and Patching</td>
</tr>
<tr>
<td>01 75 00</td>
<td>Starting and Adjusting</td>
</tr>
<tr>
<td>01 77 19</td>
<td>Closeout Requirements</td>
</tr>
</tbody>
</table>

## DIVISION 08 – OPENINGS

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>08 71 00</td>
<td>Door Hardware</td>
</tr>
</tbody>
</table>
## DIVISION 26 – ELECTRICAL
- 26 05 00 Common Work Results for Electrical
- 26 05 19 Low-voltage Electrical Power Conductors and Cables
- 26 05 26 Grounding and Bonding for Electrical Systems
- 26 05 29 Hangers and Supports for Electrical Systems
- 26 05 33 Raceways and Boxes for Electrical Systems
- 26 05 53 Identification for Electrical Systems

## DIVISION 28 – ELECTRONIC SAFETY AND SECURITY
- 28 05 00 Common Work Results for Electronic Safety and Security
- 28 05 13 Conductors and Cables for Electronic Safety and Security
- 28 50 00 Security Management System

END OF TABLE OF CONTENTS
DIRECTORY/CERTIFICATIONS

Security Implementation for Pima Community College
NTD Project No. 2009-0118-01

PROJECT

Pima Community College
District Office
4905 East Broadway Blvd.
Tucson, AZ 85709-1010
(520) 206-4500

OWNER

NTD Architects
2940 North Swan Road, Suite 214
Tucson, AZ 85712
(520) 784-0975
(520) 784-0964 FAX

ARCHITECT

ELECTRICAL
Monrad Engineering
1926 East Ft Lowell
Suite 200
Tucson, AZ 85719-2391
(520) 884-0045

CONSULTANTS

Security Implementation
Pima Community College
NTD # 2009-0118-01

DIRECTORY/CERTIFICATIONS
D - 1
PART 1 - GENERAL

1.1.1. Summary of work under this contract

1.1.2. Regulatory Requirements

1.1.3. Contractor use of site and premises.

1.1.4. Owner occupancy.

1.1.5. Work Sequence.

1.2. SUMMARY OF WORK

1.2.1. Work under this contract includes the following task areas, as shown on the drawings, specified in the Project Manual, and defined in the project contract documents, including but not necessarily limited to:

1.2.1.1. Pima Community College intends to purchase and have installed, as a turn-key project, a District-wide system for Proximity Card access and event recording of certain doors at assorted Campuses. The work includes the installation of the necessary hardware, software licensing, and miscellaneous work, demolition, and repair.

1.2.1.2. Single Source of Responsibility: Pima Community College seeks equipment and installation that is designed, assembled, packaged, and installed by a single manufacturer. The Owner expects the successful manufacturer and their approved Value Added Resource (VAR) to take responsibility for all phases of the work, from demolition through installation to warranty operations and service.

1.2.1.3. Qualification Based Procurement: PCC anticipates that the use of Proximity Cards will expand, both for the number of doors, and users assigned, but also for increased and varied functions. To facilitate that end, this is a qualification-based procurement. While a price will be required for the scope of the described installation, it will only be one of many factors the College Committee will consider in awarding the contract.

1.2.1.4. Not Used

1.2.1.5. Proposals should specifically address the following areas:

1.2.1.5.1. Vertical Scaling of the systems: One example of vertical scaling is the hardware and software increments as the number of doors increase.
1.2.1.5.2. Horizontal Scaling of the systems: PCC is aware of the wide and varied uses of Proximity Cards at other institutions. Demonstrate experience in providing for and implementing these uses. Discuss what costs and responsibilities PCC might anticipate.

1.2.1.5.3. Provisions for Redundant Systems: PCC does not desire redundancy for the current installation. However, as the system expands to perform more tasks, a redundant server at a remote location may be required. Discuss how this would be addressed and the associated costs for hardware, software and licensing.

1.2.1.5.4. When and if the system is expanded to provide cards for students, badge stations at each campus will be necessary. Discuss this issue and the necessary provisions and equipment.

1.2.1.5.5. Incremental or Unit Costs: This contract provides for Unit Pricing on certain items of expansion.

1.2.1.5.6. Schedule: Address the time you anticipate to make submittals, obtain the required equipment and complete this work.

1.2.1.5.7. Relationship of the Manufacturer and VAR:

1.2.1.5.7.1. Describe the specifics of the relationship.

1.2.1.5.7.2. Discuss how warranty and maintenance work will be performed.

1.2.1.5.7.3. Describe availability of your workforce and costs, if any, for emergency or off-hour work.

1.2.1.5.7.4. Describe what measures are taken to warehouse materials and/or expedite delivery in the case of an emergency.

1.2.1.5.7.5. Which entity will contract with PCC?

1.2.1.5.8. References: Provide a list of references with whom the Proposer’s team has done similar service. Ideally this will be a public entity and a multi-year contract. Confirm names, phone numbers and addresses before including them. Provide the names of people authorized to address your capabilities, contract and performance.

1.2.2. Perform all work in accordance with the requirements of the General Conditions and related Contract Documents.

1.3. REGULATORY REQUIREMENTS.

1.3.1. The Owner will not require building permits or regulatory review of this work.

1.3.2. Perform Work in accordance with the applicable provisions of local Codes and Regulations, including the following as adopted by jurisdictional authority.
1.3.2.1. ICBO 2009 Edition, with COT Amendments

1.3.2.2. Uniform Mechanical Code.

1.3.2.3. Uniform Plumbing Code.

1.3.2.4. National Electrical Code.

1.3.3. During the entire construction period, it shall be the sole responsibility of the Contractor to maintain conditions at the Project Site(s) to meet the requirements of the Federal Occupational Safety and Health Administration (OSHA). This provision shall cover the Contractor’s employees and all other persons working upon or visiting the site. The Contractor shall become fully informed of all applicable standards and regulations and inform all persons and representatives responsible for work under this Contract.

1.4. CONTRACTOR USE OF SITE(S) AND PREMISES

1.4.1. Contractors use of site and premises shall allow:

1.4.1.1. Work by Others and Work by Owner.

1.4.1.2. Use of site and premises by public.

1.4.2. Access to Site: Coordinate with Owner.

1.4.3. Building Exits During Construction: Maintain all exits. Do not obstruct at any time.

1.4.4. Time and Construction Schedule Considerations:

1.4.4.1. Schedule all construction operations with Owner.

1.4.4.2. Construction operations generating excessive noise, such as use of pneumatic tools and powder actuated fastener equipment, shall be scheduled with the Owner.

1.4.4.3. Locate all noise generating equipment, such as cut-off saws, in a remote location away from administrative or classroom areas.

1.4.4.4. Owner reserves the right to modify such scheduled operations to accommodate school operations or classroom programs.

1.4.4.5. Provide Owner with 10 working days notice prior to commencing operations at each Campus.

1.4.4.6. After Owner takes beneficial occupancy of portions of project the Contractor, subcontractors and all support staff will not be allowed to enter such school facilities during hours school is in session. Where access is required to complete the work, coordinate access and scheduling with Owner’s representative for non-school time.

1.4.4.7. No interference with classroom or administrative activities will be permitted without approval of Owner’s Project Manager.

1.4.5. Corporation Yard and Storage Areas: Coordinate with Owner. Coordinate location with areas required by work performed under separate contract by others. Owner will establish acceptable path for products, staging areas, and trash disposal.
1.4.5.1. Coordinate location of all equipment parking, material and stockpile storage and construction parking with Owner.

1.5. OWNER OCCUPANCY

1.5.1. The Owner will occupy the site and existing facilities during entire period of construction for the conduct of normal school and business operations.

1.5.2. Cooperate with Owner to minimize conflict, and to facilitate Owner's operations.

1.6. FEES, BONDS, AND PERMITS

1.6.1.1. None required.

2. PART 2 - PRODUCTS

\Not Used

3. PART 3 - EXECUTION

\Not Used

END OF SECTION
1. **PART 1 – GENERAL**

1.1. **SECTION INCLUDES**

1.1.1. In order to allow the Owner to determine in advance the additional costs for additional work, certain Unit Prices are defined below.

1.1.2. The proposed Unit Price for each of the items shall be reflected on the Bid Form and as described.

1.1.3. Unit Prices defined shall be used in determining the cost to the Owner of work items added to or deleted from the scope of the work as shown on the drawings. The cost of all other work shall be included in the Contract Lump Sum stipulated on the Bid Form.

1.1.4. Unit Pricing shall remain in force for the construction period and for the first year of the maintenance agreement period. At the end of each successive year, assuming the contract is renewed, the amounts will be re-negotiated.

1.2. **RELATED WORK DESCRIBED ELSEWHERE**

1.2.1. Pertinent sections of these Specifications describe the materials and methods required under the various Unit Prices.

1.2.2. The method for stating the proposed Unit Prices is described on the Bid Form.

1.3. **SUBMITTALS**

1.3.1. All Unit Prices described in this Section are required to be reflected in the bid submitted on the bid form for the work. Do not submit other pricing approaches.

1.4. **MEASUREMENT AND PAYMENT**

1.4.1. General

1.4.1.1. If the Owner elects to make modifications to the work that involves items defined by the Unit Price schedule, the Agreement shall be modified by Change Order procedures defined in the General and Supplementary Conditions.

1.4.2. Measurement

1.4.2.1. Documentation required by the Change Order procedures shall include substantiation of quantities associated with Unit Prices, including invoicing, area take-offs, and related data.

1.4.2.2. The Owner reserves the right to prepare independent audit of quantities proposed by Contractor.

1.4.2.3. Unit Prices shall be the total price and include all labor, material, subcontractor and general contractor supervision, overhead and profit.
1.4.3. Payment

1.4.3.1. If made done the original construction period, costs associated with Unit Price items shall be incorporated into Change Order modifications to the Agreement. If made subsequent to the original construction, the Owner will issue a purchase order.

1.4.3.2. Payment for Change Orders shall be per procedures defined in the General and Supplementary Conditions.

2. PART 2 - PRODUCTS

2.1. UNIT PRICE SCHEDULE

2.1.1. Item Number (1): Card Reader and associated equipment including door hardware modifications. Provide Unit Cost for the addition of new readers and associated wiring and an adjacent ceiling junction box for additional doors. Unit price is to include up to 150 feet of cabling to the System Recorder. Modify software as required to include the new door(s) in the monitoring system.

2.1.2. Item Number (2): Wiring from ceiling junction box to control panel. Provide Unit Cost for the addition of required wiring to operate reader and hardware in increments of 25 feet of run, regardless of the pathway. This in excess of the 150 allowed for in 2.1.1.

2.1.3. Item Number (3): Additional two-door interface module compatible with the Intelligent System Recorder and all associated wiring and software.

2.1.4. Item Number (4): Additional Proximity Card Blanks. Provide Unit Cost for the additional blank access cards, in increments of 25 cards.

3. PART 3 - EXECUTION

3.1. COORDINATION

3.1.1. Thoroughly and clearly advise all necessary personnel and suppliers as to the nature and extent of Unit Price contract adjustments selected by the Owner. Use all means necessary to coordinate those personnel and suppliers involved as to all changes in the Work.

END OF SECTION
SECTION 01 26 00
CONTRACT PROCEDURES

1. PART 1 - GENERAL

1.1. SECTION INCLUDES

1.1.1. Application for Payment and Schedule of Values.

1.1.2. Contract Document modification procedures, including contract change orders.

1.1.3. Request for Information Procedures.

1.2. SCHEDULE OF VALUES

1.2.1. Submit typed Application for Payment and Schedule of Values on A.I.A. forms G702 and G703 complying with the format established in this Section. Contractor's standard form or electronic print-out format may be considered, at Architect's discretion.

1.2.2. Correlate line items with terms and identification used in other administrative work items, including schedules, list of subcontractors, list of products and suppliers, and submittal schedule.

1.2.3. Provide schedules as follows.

1.2.4. The total of the amounts of all scheduled line items shall equal the Contract Sum. Round amounts to nearest dollar.

1.2.5. Revise schedule to list approved Change Orders and Construction Change Directives, and submit with each Application For Payment.

1.2.6. The amounts shown on Schedule of Values may be used by Owner to determine the true value for additive or deductive change orders.

1.3. CHANGE PROCEDURES

1.3.1. General

1.3.1.1. Contractor shall establish measures as needed to assure familiarity of the Contractor's staff and employees with procedures for processing changes to the Contract Documents.

1.3.1.2. The Contractor shall maintain and coordinate a Register of RFI’s, ASI’s, Contractor Change Order Requests, CCD’s and Change Orders at the job site, accurately reflecting current status of all pertinent data as submitted by the Contractor.

1.3.2. Architect's Supplemental Instructions (ASI): The Architect will advise of minor changes in the Work that do not involve an adjustment to Contract Price or Contract Time by issuing supplemental instructions on AIA Form G710 or other Architect issued document.
1.3.2.1. If Contractor considers the minor change does represent a change in the contract, Contractor shall immediately notify the Architect of Contractor's intention to make a claim.

1.3.3. Proposal Request (PR): The Architect may issue a Proposal Request which includes a detailed description of a proposed change with supplementary or revised Drawings and specifications.

1.3.3.1. Analyze the described change and its impact on costs and time. Submit response within 10 days. If accepted by Owner, Architect will prepare Change Order.

1.3.3.2. When requested, meet with the Architect as required to explain costs and, when appropriate, determine other acceptable ways to achieve the desired objective.

1.3.3.3. Alert pertinent personnel and subcontractors as to the impending change and, to the maximum extent possible, avoid such work as would increase the Owner's cost for making the change, advising the Architect in writing when such avoidance no longer is practicable.

1.3.3.4. Following review, and if accepted by Owner, Architect will prepare Change Order.

1.3.4. Change Order Request (COR):

1.3.4.1. Contractor may submit a COR to the Architect for changes in conditions, Owner changes, or other direction from the Architect, jurisdictional authority or Owner's inspector.

1.3.4.2. Document the proposed change and its complete impact, including its effect on the cost and schedule of the work.

1.3.4.3. Present total cost and schedule impacts in documentation, including all mark-ups permitted by General Conditions. Provide detailed back-up as required by Architect, including supplier costs, sub-contractor labor time and rates, and all other data deemed necessary by Architect for Owner's and Architect's review of COR.

1.3.4.4. Following final review by Architect and Owner of original and supplemental information, and if COR is accepted, no additional cost or schedule adjustments will be included.

1.3.4.5. Architect will review COR. If accepted, Architect will prepare a Change Order or Construction Change Directive.

1.3.5. Change Order (CO): Change Orders and Construction Change Directives will be issued by the Architect in accordance with procedures established in General Conditions.

1.3.5.1. Change Order Forms: NTD form.

1.3.5.2. Execution of Change Orders: Architect will issue Change Orders for signatures of Owner, Architect, and Contractor as provided in the General Conditions of the Contract.
1.3.6. Architect will provide a single copy of all documents issued under this Article for transmission to Contractor. Contractor shall prepare copies as required for distribution to subcontractors, suppliers and others at no cost to Owner.

1.4. PROGRESS PAYMENT COORDINATION

1.4.1. Submit application on AIA Form G702-Application and Certificate for Payment as follows:

1.4.1.1. Submit initial rough draft of pay application to Architect, Inspector of Record and Owner for review.

1.4.1.2. Architect will return initial rough draft of pay application to Contractor following review.

1.4.1.3. Submit three (3) copies of adjusted pay application to Architect.

1.4.1.4. Submit conditional lien releases for work covered by current application, and unconditional releases for work covered by previous months billings.

1.4.2. Content and Format: Utilize Schedule of Values for listing items in Application for Payment.

1.4.3. Payment Period: Monthly, scheduled as defined in General Conditions.

1.4.4. Application Preparation:

1.4.4.1. Complete every entry on the form, including notarization and execution by person authorized to sign legal documents on behalf of the Contractor. Incomplete applications will be returned without action.

1.4.4.2. Transmit each copy with a transmittal form listing attachments, and recording appropriate information related to the application in a manner acceptable to the Architect.

1.4.4.3. Entries shall match data on the Schedule of Values and Contractor's Construction Schedule. Use updated schedules if revisions have been made. Include amounts of Change Orders and Construction Change Directives issued prior to the last day of the construction period covered by the application.

1.5. PAYMENT FOR CONTRACT DOCUMENT MODIFICATIONS

1.5.1. The Contractor shall compensate the Owner, by Owner-Contractor Contract adjustment, for the Architect reasonable costs to modify Contract Documents required by work not performed in accordance with approved Contract Documents.

1.6. REQUEST FOR INFORMATION

1.6.1. The Architect will respond to legitimate and bonafide Requests for Information (RFI) initiated by Contractor.

1.6.2. Submit all RFI's on attached form. Use of Contractor's form will not be accepted. RFI's submitted by subcontractors or suppliers will not be reviewed.
1.6.3. The Contractor shall compensate the Architect, by Owner-Contractor Contract adjustment, for the Architect's reasonable costs to respond to RFI's if the Architect determines:

1.6.3.1. The RFI does not reflect careful study and review of the documents, or;

1.6.3.2. Demonstrates a lack of knowledge or construction competency reasonably expected of a Contractor performing the work.

1.6.4. The Architect's action will be taken with such reasonable promptness while allowing sufficient time in the Architect's professional judgment to permit adequate review.

1.6.5. RFI's received in Architect's office after 9:00 AM Friday will be logged in as received by Architect on Monday, 8:00 AM. This applies to all forms of communication, including RFI's arriving via FAX transmission.

2. PART 2 - PRODUCTS

\Not Used

3. PART 3 - EXECUTION

\Not Used

END OF SECTION
CONTRACTOR'S REQUEST FOR INFORMATION

From: _____________________________________  NTD Proj. # ________  Date: ___________

To: _____________________________________  NTD Project: ____________________________

Disciplines Impacted:
[ ] Structural  [ ] Mechanical  [ ] Electrical  [ ] Architectural
[ ] Civil  [ ] Landscape  [ ] Kitchen  [ ] ______________________________

Reference: Drawing(s) ____________  Spec Section(s) ____________  Other ______________

Please clarify or provide the following information:
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________

Possible Cost Impact
[ ] Increase  [ ] Decrease  [ ] No Change  [ ] Unknown

Possible Time Impact
[ ] Increase  [ ] Decrease  [ ] No Change  [ ] Unknown

This information is required as soon as possible, but no later than__________________________

[ ] PRIORITY ATTENTION REQUIRED

Copies to: _________________________

Contractor's Representative

Architect's Response:  Date: ___________

__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________

Copies to: _________________________

NTD Representative
SECTION 01 33 00
SUBMITTAL PROCEDURES

1. PART 1 - GENERAL

1.1. SECTION INCLUDES

1.1.1. Submittal procedures.

1.1.2. Proposed Products list.

1.1.3. Shop drawings.

1.1.4. Product data.

1.1.5. Samples.

1.1.6. Manufacturers' instructions.

1.1.7. Manufacturers' certificates.

1.2. SUBMITTAL PROCEDURES

1.2.1. Transmit required submittals to Architect per criteria in the General Conditions and as specified.

1.2.1.1. Transmit submittals within time periods established by the General Conditions and as required to maintain orderly and sequential progress of the work.

1.2.1.2. Maintain complete and current submittal log, indicating status of all submittals and re-submittals. Provide summary of submittal status at pay request meeting.

1.2.2. Failure to make timely submittals will not be reason for extension of Contract Time.

1.2.3. Architect's review of submittals shall not relieve the Contractor for compliance with the Contract Documents, or for responsibility for deviations from Contract Documents.

1.2.3.1. In review of submittals, Architect will not provide dimensions or elevations for field conditions, or for conditions available from a detailed review of documents.

1.2.4. Electronic Documents for Contractors Use.

1.2.4.1. At Architect's sole discretion, Architect will provide a file containing selected electronic file backgrounds for Contractor's use in shop drawing preparation.

1.2.4.2. Contractor shall sign Architect provided release form regarding such electronic file information.
1.2.4.3. Electronic files will be provided in AutoCAD format, in the Architect's current version, as background views only, without dimensions, doors, notes and similar information. No seals, title blocks or approval stamps will be included on backgrounds.

1.2.4.4. Unless otherwise established, and at Architect's sole discretion, only plan and section views of architectural, structural, mechanical, and electrical documents will be provided. Under no circumstances will the complete project AutoCAD file be provided.

1.2.4.5. The Architect will provide a single CD based file containing backgrounds for all discipline for the contractor's use. Contractor shall be responsible for distribution of background files to subcontractors and vendors.

1.2.4.6. The Architect will prepare a cost for preparation of electronic file package. If the Contractor agrees to such cost, the cost will be processed as a deductive change order to the contract.

1.2.5. Copying of Contract Documents for use as submittals is not acceptable. Contractor shall produce original documents for shop drawings and other submittals.

1.2.6. Provide submittals within the following time periods and as required for the orderly progress of the work. Where no time period is established, provide submittals no later than the midpoint between notice of award and scheduled start date of the work related to the submittal. Where submittals are not submitted within specified limits, the Architect may delay certification of Payment Request until submittals are received.

1.2.7. The Architect's action will be taken within a reasonable time period, while allowing sufficient time, in the Architect's professional judgment, to permit adequate review.

1.2.8. Transmit each submittal separately with Architect accepted form.

1.2.8.1. Combine required material for a single specification Section into a single submittal. Incomplete or partial submittals will be returned without action for re-submittal in proper form.

1.2.8.2. Do not combine data from more than one specification section or drawing component into a single submittal. Such submittals received will be returned without action for re-submittal in proper form.

1.2.8.3. Submittals not reviewed by General Contractor will be returned without action for proper review and re-submittal.

1.2.9. Submittal Procedure:

1.2.9.1. All submittals, other than actual product samples, are to be submitted electronically in an Adobe PDF format. Architect will review and return as an Adobe PDF.

1.2.9.1.1. Prior to starting submittals, representatives of the Architect and Contractor will meet to establish protocols and agree on specific software for use in the submittal process.

1.2.10. Sequentially number the transmittal forms. Re-submittals to have original number with an alphabetic or numeric suffix.
1.2.11. Identify Project, Contractor, Subcontractor or supplier; pertinent Drawing sheet and detail number(s), and specification Section number, as appropriate.

1.2.12. Apply Contractor's stamp, signed or initialed certifying that review, verification of Products required, field dimensions, adjacent construction Work, and coordination of information, is in accordance with the requirements of the Work and Contract Documents.

1.2.13. Schedule submittals to expedite the Project, and deliver to Architect at business address. Coordinate submission of related items.

1.2.14. Identify variations from Contract Documents and Product or system limitations which may be detrimental to successful performance of the completed Work.

1.2.14.1. Clearly identify, with bold clouding, or other graphic notation, all deviations from Contract Documents. Provide boxed note at clouded deviation specifically requesting approval of proposed change. Provide documentation of proposed change, including additional graphics and data as required by Architect.

1.2.15. Provide space for Contractor and Architect review stamps.

1.2.16. Revise and resubmit submittals as required, identify all changes made since previous submittal.

1.2.16.1. Provide re-submittals within seven days of receipt of returned submittal.

1.2.17. Distribute copies of reviewed submittals to concerned parties. Instruct parties to promptly report any inability to comply with provisions.

1.2.17.1. Distribute all copies of reviewed submittals at no additional cost to Owner for duplication, blueprinting, mailing or other costs.

1.2.18. Do not send submittals unless required by Specification. Submittals transmitted to Architect not required by specification will be returned without review.

1.2.19. Architect will notify Contractor of availability of documents for pickup at Architect's office, and log such date as the date returned to Contractor. Architect is not obligated to transmit or deliver submittals to Contractor.

1.2.20. Samples: Provide samples as specified in each Section.

1.2.21. Manufacturer's Data: Provide descriptive data on all accessory items and operation.

1.2.22. Installation Data: Submit descriptive data on installation procedures.

1.3. PROPOSED PRODUCTS LIST AND PRODUCT DATA

1.3.1. Where specified in individual sections, submit complete list of major products proposed for use, with name of manufacturer, trade name, and model number for each product and supporting product data.

1.3.1.1. For products specified only by reference standards, give manufacturer, trade name, model or catalog designation, and reference standards.

1.3.2. Provide data electronically in PDF format.
1.3.3. Mark submittal to identify applicable products, models, options, and other data. Supplement manufacturers’ standard data to provide information unique to this Project. Mark out items that are not applicable to the project.

1.3.4. After review, distribute in accordance with this Section and provide copies for Project Record Documents described in Section 01 77 19 – Closeout Requirements.

1.4. SHOP DRAWINGS

1.4.1. Submit in the form defined in the General Conditions and as specified.

1.4.1.1. Submit shop drawings in black or colored image on white bond paper format – blue print copies are not acceptable.

1.4.2. Submittal Procedure:

1.4.2.1. All submittals, other than actual product samples, are to be submitted electronically in an Adobe PDF format. Architect will review and return as an Adobe PDF.

1.4.2.1.1. Prior to starting submittals, representatives of the Architect and Contractor will meet to establish protocols and agree on specific software for use in the submittal process.

1.4.2.2. Architect will return one copy of marked up and stamped shop drawing to Contractor.

1.4.3. Provide the following information on each sheet:

1.4.3.1. Project name and location.

1.4.3.2. Contractor name and address.

1.4.3.3. Subcontractor, manufacturer, or fabricator name and address.

1.4.3.4. Date and scale of drawings

1.4.3.5. Space for Contractor's review and approval stamp.

1.4.4. After review, reproduce and distribute in accordance with this Section and as described for Project Record Drawings in Section 01 77 19 – Closeout Requirements.

1.5. MANUFACTURER'S INSTRUCTIONS AND CERTIFICATES

1.5.1. When specified in individual specification Sections, submit manufacturers certificates and instructions for delivery, storage, assembly, installation, start - up, adjusting, and finishing, in quantities specified for Product Data.

1.5.2. Identify conflicts between manufacturers' instructions and Contract Documents.

1.5.3. Indicate material or Product conforms to or exceeds specified requirements. Submit supporting reference data, affidavits, and certifications as appropriate.

1.5.4. Certificates may be recent or previous test results on material or Product, but must address current regulatory requirements and be acceptable to Architect.
1.6. SAMPLES

1.6.1. Submit samples to illustrate functional and aesthetic characteristics of the Product, with integral parts and attachment devices. Coordinate sample submittals for interfacing work.

1.6.2. Include identification on each sample, with full Project information.

1.6.3. Submit the number of samples of selected finish color, texture, and pattern as specified in individual specification Sections, with a minimum of five samples provided. Where multiple samples are specified, the Architect will retain four sets.

1.6.4. Submittal Procedure for Color Section:

1.6.4.1. Initial Submittal: Using manufacturers standard sample delivery system, submit two sets of samples of colors and finishes from the full range of manufacturers' standard colors (and custom colors if specified), textures, and patterns for Architect initial selection.

1.6.4.2. The Architect will notify Contractor of initial selection by ASI.

1.6.4.3. Following receipt of initial selection, submit the number of samples of selected finish color, texture, and pattern as specified in individual specification Sections, with a minimum of five samples provided. Where multiple samples are specified, the Architect will retain three sets.

1.7. SUBSTITUTIONS

1.7.1. Substitutions will be considered in accordance with the General Conditions and Section 01 25 00.

1.7.2. Substitutions will not be considered when indicated or implied on shop drawings or other forms of submittal without separate written request for substitution.

2. PART 2 - PRODUCTS

Not Used

3. PART 3 - EXECUTION

Not used

END OF SECTION
SECTION 01 50 00
TEMPORARY FACILITIES AND CONTROLS

1. PART 1 - GENERAL

1.1. SECTION INCLUDES

1.1.1. Temporary Utilities: Contractor may use PCC electrical outlets, water, and sanitary facilities. Contractor may not use PCC telephone or data service.

1.1.2. Temporary Controls: Barriers, enclosures and fencing, protection of the Work, and related operational requirements.

1.1.3. Construction Facilities: Access, parking, and progress cleaning.

1.2. TEMPORARY ELECTRICITY

1.2.1. Owner will pay cost of energy used. Exercise measures to conserve energy. Connect to existing power service. Power consumption shall not disrupt Owner's need for continuous service. Coordinate location of connection with Owner.

1.2.2. Provide all required disconnects, overcurrent protection devices, and power cords as required for the Work.

1.2.3. Permanent convenience outlets may be used during construction.

1.3. TELEPHONE/FAX/COPY/DATA SERVICE

1.3.1. Provide, maintain and pay for cellular phone and data service for the on-site Superintendent.

1.4. TEMPORARY WATER SERVICE

1.4.1. Use of on-site existing water service for potable drinking water is acceptable. Coordinate point of connection with Owner.

1.5. TEMPORARY SANITARY FACILITIES

1.5.1. Use of existing toilet facilities, or toilets is permitted. Contractor shall monitor his workforce behavior.

1.6. BARRIERS AND BARRICADES

1.6.1. Provide barriers to prevent unauthorized entry to construction areas, to allow for Owner's use of site, and to protect existing facilities and adjacent properties from damage from construction operations and demolition.

1.6.1.1. When regulated by codes, such legal requirements for protection shall be considered as minimum requirements. Provide protective measures in excess of such minimum requirements as specified or required.

1.6.1.2. Protect non-owned vehicular traffic, stored materials, site and structures from damage.
1.6.2. Interior

1.6.2.1. After beneficial occupancy, and where required to permit Owners on-going operations, provide barriers.

1.6.2.2. Protect existing surfaces, equipment and furnishings from damage from construction operations and demolition. Where necessary, remove and store in separate area.

1.6.2.3. Where demolition or construction operations generate fine dust or air-borne particulates, provide fire retardant drop cloths, screening or other approved barriers to prevent dust intrusion into existing cabinet interiors, equipment, drawers, and similar conditions.

1.7. PROTECTION OF INSTALLED WORK

1.7.1. Protect installed Work and provide special protection where specified in individual specification Sections.

1.7.2. Provide temporary and removable protection for installed Products. Control activity in immediate work area to minimize damage.

1.7.3. Provide protective coverings at walls, projections, jambs, sills, and soffits of openings.

1.7.4. Provide and maintain all required dams, screens and collection systems necessary to prevent water used in interior demolition or construction operations from damaging adjacent areas.

1.7.5. Take all means required to prevent damage to project, including interior areas, resulting from inclement weather, water, wind or other environmental impacts. Provide temporary coverings or enclosures as required for all roof and wall penetrations. Where moisture from condensation, rain or high winds is forecast or present, Contractor shall take all means to eliminate or prevent danger to the Work and to adjacent property, including covering unprotected surfaces, making all openings weather tight, removing loose materials, tools or equipment from exposed locations and removing or securing scaffolding.

1.8. PARKING AND TRAFFIC CONTROL

1.8.1. Parking Criteria

1.8.1.1. Coordinate location and number of parking spaces to be made available for Contractors forces with Owner.

1.8.1.2. Do not permit parking on adjacent public streets.

1.8.1.3. Provide and maintain access to fire lanes and fire hydrants at all times, free of obstructions.

1.8.2. Do not permit delivery trucks to block, park or wait on public streets.

1.8.3. Coordinate site access through locked access gates with Owner. Keys to such gates will not be released to Contractor.
1.9. PROGRESS CLEANING

1.9.1. Maintain areas free of waste materials, debris, and rubbish. Maintain site in a clean and orderly condition.

1.9.2. Use cleaning materials which do not create hazards to health or property and which will not damage surfaces. Use only those cleaning materials and methods recommended by manufacturer of the surface material to be cleaned. Use cleaning materials only on surfaces recommended by cleaning material manufacturer.

1.9.3. Remove debris and rubbish from pipe chases, plenums, attics, crawl spaces, and other closed or remote spaces, prior to enclosing the space.

1.9.4. Broom and vacuum clean interior areas prior to start of surface finishing, and continue cleaning to eliminate dust.

1.9.5. Remove waste materials, debris, and rubbish from interior spaces daily and deposit in approved PCC dumpster. Remove from site daily.

1.9.6. Broom and vacuum clean interior areas prior to start of all surface finishing, including painting, and continue cleaning on an as-needed basis until painting and surface finishes are complete.

1.9.7. Schedule operations so that dust and other contaminants resulting from cleaning procedures or construction operations will not fall on wet or newly-coated surfaces.

1.10. FIELD OFFICES AND SHEDS

1.10.1. Project Office: Coordinate with Owner the use and maintenance of existing interior space for field office purposes.

1.10.2. Determine office location at each campus as directed by Owner.

1.10.3. Architect, Owner, and their representatives shall have free access to the Owners and Inspectors office at all times.

1.10.4. Furnish, install and maintain tool cribs, sheds and storage units for the Contractors use as necessary for the proper execution of the work. Locations shall be approved by Owner.

1.10.4.1. Return all small tools and secure in locked compartments or cribs at close of work day.

1.10.4.2. Safe-off or lock all equipment and large tools. Disable from malicious or accidental start-up and operation.

1.10.4.3. Storage facilities shall provide protection of all products from damage due to environmental conditions, abuse, or theft.

1.10.5. Requirements of regulatory agencies: Comply with requirements of regulatory agencies having jurisdiction. Obtain and apply for permits required by governing authorities.

1.10.6. Job Conditions: Locate temporary structures to avoid interference with Work. Relocate temporary structures as required by job progress.
1.11. RECORD DOCUMENTS: JOB SET

1.11.1. Contractor shall maintain, on site, one copy of the following contract documents, defined as the Record Job Set. Stamp set “RECORD JOB SET - DO NOT REMOVE”. During the course of construction, use this set to record actual revisions to the Work.

1.11.1.1. Construction Drawings.
1.11.1.2. Project Manual/Specifications.
1.11.1.3. Addenda.
1.11.1.4. Change Orders and other Modifications to the Contract.
1.11.1.5. Reviewed shop drawings, product data, and samples.

1.11.2. Store Record Job Set separate from documents used for construction.

1.11.3. Transfer information concurrent with construction progress. Record Job Sets will be reviewed at each Progress Meeting.

1.11.3.1. Where Record Job Sets do not reflect actual field conditions, the Architect may delay certification of Payment Request until sets are updated to the Architects satisfaction.

1.11.4. Specifications: Legibly mark and record at each Part 2 Product section description of actual Products installed, including the following:

1.11.4.1. Manufacturer’s name and product model and number.
1.11.4.2. Product substitutions or alternates utilized.
1.11.4.3. Changes made by Addenda and Modifications.
1.11.4.4. Details not on original Contract Drawings.

1.12. REMOVAL OF UTILITIES, FACILITIES, AND CONTROLS

1.12.1. Remove temporary utilities, equipment, facilities, and materials, prior to Final Application for Payment.

1.12.2. Clean and repair damage caused by installation or use of temporary work.

1.12.3. Restore existing facilities used during construction to original condition. Restore permanent facilities used during construction to specified condition.

1.13. SECURITY

1.13.1. Provide security and facilities as necessary to protect work and personnel from vandalism, unauthorized entry, theft, damage, or assault.

1.13.2. Where Owner has given approval to take fire detection system off-line, return system to active status at completion of work or end of each work period.
1.13.2.1. Where security or fire detection systems are disabled for any reason, including where Owner has given approval for such system shut-down, provide fire watch or security guard service as directed by Owner and at no additional cost to the Owner.

1.13.3. All Contractor staff, subcontractors and suppliers shall present a professional and civil manner to staff, visitors, neighbors and students. Use of language or behavior judged offensive, obscene or suggestive by the Owner is not permitted. Clothing that is suggestive, is marked with images that suggest or promote drug, alcohol or tobacco use, or represents behavior judged offensive, obscene or suggestive by the Owner is not permitted. Immediately remove from site campus any Contractor personnel exhibiting such behavior.

1.14. DOCUMENTATION OF EXISTING CONDITIONS

1.14.1. Prior to beginning any alterations, including wall demolition or fixture removal, prepare a record of existing improvements affected by the work of this contract.

1.14.1.1. Prepare record document using digital color video, recorded on DVD, and any other means of documentation necessary to describe existing condition.

1.14.1.2. Obtain Owners’ Inspector of Record certification that documents were prepared prior to beginning construction. Deliver DVD and associated documentation to Owner prior start of construction.

1.15. USE OF ELEVATORS (WHERE PROVIDED)

1.15.1. Coordinate all use of all existing elevators for construction operations with Owner. Owner will designate specific elevators for use during construction period.

1.15.2. Protect interior wall surfaces with pads and flooring with removable sheet goods.

1.15.3. Remove protective pads and floor covering and vacuum clean interior after each period of use.

2. PART 2 – PRODUCTS

Not Used

3. PART 3 - EXECUTION

Not Used

END OF SECTION
SECTION 01 73 29
CUTTING AND PATCHING

1. PART 1 - GENERAL

1.1. SECTION INCLUDES

1.1.1. Requirements and limitations for cutting and patching of Work.

1.2. QUALITY ASSURANCE

1.2.1. Use only personnel who are thoroughly trained and experienced in the skills required and have installed similar applications of the specified products within one year prior to beginning work of this section.

1.2.2. Use only staff who are completely familiar with the requirements of this work.

1.3. DEFINITIONS

1.3.1. Cutting: Removal of in-place construction necessary to permit installation or performance of other Work.

1.3.2. Patching: Fitting and repair work required to restore surfaces to original conditions after installation of other Work.

1.4. SUBMITTALS

1.4.1. Cutting and Patching Proposal: Submit a proposal describing procedures at least 5 days before the time cutting and patching will be performed, requesting approval to proceed. Include the following information:

1.4.1.1. Extent: Describe cutting and patching. Show how they will be performed. Indicate why they cannot be avoided.

1.4.1.2. Changes to In-Place Construction: Describe anticipated results. Changes to structural elements and operating components are not permitted. Describe changes in building's appearance and other significant visual elements.

1.4.1.3. Products: List products to be used and firms or entities that will perform the Work.

1.4.1.4. Utility Services and Mechanical/Electrical Systems: List services/systems that cutting and patching procedures will disturb or affect. List services/systems that will be relocated and those that will be temporarily out of service. Indicate how long services/systems will be disrupted.

1.4.1.5. Architect's Approval: Obtain approval of cutting and patching proposal before cutting and patching. Approval does not waive right to later require removal and replacement of unsatisfactory work.
1.5. QUALITY ASSURANCE

1.5.1. Structural Elements: Do not cut and patch structural elements. Operational Elements: Do not cut and patch operating elements and related components in a manner that results in reducing their capacity to perform as intended or that results in increased maintenance or decreased operational life or safety. **Operating elements include the following:**

1.5.1.1. Primary operational systems and equipment, including mechanical, plumbing, fire protection, electrical and data/communication systems.

1.5.1.2. Air or smoke barriers.

1.5.1.3. Conveying systems.

1.5.1.4. Electrical wiring systems.

1.5.1.5. Operating systems of special construction in Division 13 Sections.

1.5.2. Miscellaneous Elements: Do not cut and patch miscellaneous elements or related components in a manner that could change their load-carrying capacity, that results in reducing their capacity to perform as intended, or that results in increased maintenance or decreased operational life or safety. These include but are not limited to:

1.5.2.1. Water, moisture, or vapor barriers.

1.5.2.2. Window or curtainwall assemblies.

1.5.2.3. Equipment supports.

1.5.3. Visual Requirements: Do not cut and patch construction in a manner that results in visual evidence of cutting and patching. Do not cut and patch construction exposed on the exterior or in occupied spaces in a manner that would, in Architect's opinion, reduce the building's aesthetic qualities. Remove and replace construction that has been cut and patched in a visually unsatisfactory manner.

1.5.4. Cutting and Patching Conference: Before proceeding, meet at Project site with parties involved in cutting and patching, including mechanical and electrical trades. Review areas of potential interference and conflict. Coordinate procedures and resolve potential conflicts before proceeding.

1.6. WARRANTY

1.6.1. Existing Warranties: Remove, replace, patch, and repair materials and surfaces cut or damaged during cutting and patching operations, by methods and with materials so as not to void existing warranties.

2. PART 2 - PRODUCTS

2.1. PRODUCTS FOR PATCHING AND EXTENDING WORK

2.1.1. General:

2.1.1.1. Unless noted otherwise, provide products matching existing finish, color, dimension, and assembly.
2.1.1.2. If matching materials are unavailable or cannot be used, use materials that, when installed, will match the visual and functional performance of in-place materials.

2.1.1.3. All products shall be new, unless specifically noted otherwise.

2.1.1.4. Provide asbestos-free materials.

2.1.1.5. Maintain all fire resistance ratings of existing assemblies and materials.

2.1.1.6. Maintain water and weather tight characteristics of assemblies and materials.

2.1.2. Comply with requirements as specified in applicable specification sections for materials used in repairing and extending existing work.

3. PART 3 - EXECUTION

3.1. SURFACE CONDITIONS

3.1.1. Inspection

3.1.1.1. Prior to work of this section, carefully inspect previously installed work. Verify all such work is complete to the point where this installation may properly commence.

3.1.1.2. Verify that work of this section may be installed in strict accordance with the original design, all pertinent codes and regulations, and all pertinent portions of the referenced standards.

3.1.1.3. In the event of discrepancy, immediately notify the Architect.

3.1.1.4. Do not proceed with installation in areas of discrepancy until all such discrepancies have been fully resolved.

3.1.2. During the course of the work, advise Architect of all discovered deficiencies, damage and degradation in existing structure, including finishes, and all plumbing, heating, ventilation, air conditioning, and electrical systems.

3.1.3. All cost caused by defective or ill-timed work shall be borne by Contractor. Contractor shall not endanger any work by cutting, excavating, or otherwise altering work and shall not cut or alter work of any other Contractor except with consent of Architect.

3.2. PREPARATION

3.2.1. Provide temporary supports as required to ensure structural integrity of the Work, including scaffolding, shoring, and underpinning. Provide devices and methods to protect other portions of Project from damage.

3.2.2. Utility and Service Identification and Location

3.2.2.1. Locate and identify existing utility, service and irrigation system components affected by work of this contract. Review existing record drawings, conduct site investigations, contact Underground Service Alert and other qualified on-site cable/pipe/line locator services, and implement all other means necessary to define the location of underground systems.
Prior to beginning any cutting or patching affecting identified utilities, properly disconnect all water, gas and electrical power supply at appropriate disconnect locations. Obtain all necessary releases and approvals from serving utility companies.

Prior to disconnect, obtain Owner's approval that such system does not impact facilities or systems beyond the extent of this contract.

Mark location of disconnected systems. Identify and indicate stub-out locations on Project Record Documents.

Coordinate the time and duration of all system disconnects with Owner.

Protection: Protect in-place construction during cutting and patching to prevent damage. Provide protection from adverse weather conditions for portions of Project that might be exposed during cutting and patching operations.

Adjoining Areas: Avoid interference with use of adjoining areas or interruption of free passage to adjoining areas.

3.3. **CUTTING AND PATCHING**

**3.3.1.** General: Employ skilled workers to perform cutting and patching. Proceed with cutting and patching at the earliest feasible time, and complete without delay.

Cut in-place construction to provide for installation of other components or performance of other construction, and subsequently patch as required to restore surfaces to their original condition.

Cut in-place construction by sawing, drilling, breaking, chipping, grinding, and similar operations, including excavation, using methods least likely to damage elements retained or adjoining construction. If possible, review proposed procedures with original Installer; comply with original Installer's written recommendations.

In general, use hand or small power tools designed for sawing and grinding, not hammering and chopping. Cut holes and slots as small as possible, neatly to size required, and with minimum disturbance of adjacent surfaces. Temporarily cover openings when not in use.

Cut or drill from the exposed or finished side into concealed surfaces.

Concrete and Masonry: Cut using a cutting machine, such as an abrasive saw or a diamond-core drill. Do not over-cut corners when using saws. Core drill corners and grind as required to establish square corners.

Mechanical and Electrical Services: Cut off pipe or conduit in walls or partitions to be removed. Cap, valve, or plug and seal remaining portion of pipe or conduit to prevent entrance of moisture or other foreign matter after cutting.

Proceed with patching immediately after construction operations requiring cutting are complete.
3.3.3. Patching: Patch construction by filling, repairing, refinishing, closing up, and similar operations following performance of other Work. Patch with durable seams that are as invisible as possible. Provide materials and comply with installation requirements specified in other Sections.

3.3.3.1. Inspection: Where feasible, test and inspect patched areas after completion to demonstrate integrity of installation.

3.3.3.2. Exposed Finishes: Restore exposed finishes of patched areas and extend finish restoration into retained adjoining construction in a manner that will eliminate evidence of patching and refinishing.

3.3.3.2.1. Clean piping, conduit, and similar features before applying paint or other finishing materials.

3.3.3.2.2. Restore damaged pipe covering to its original condition.

3.3.3.3. Floors and Walls: Where walls or partitions that are removed extend one finished area into another, patch and repair floor and wall surfaces in the new space. Provide an even surface of uniform finish, color, texture, and appearance. Remove in-place floor and wall coverings and replace with new materials, if necessary, to achieve uniform color and appearance.

3.3.3.3.1. Where patching occurs in a painted surface, apply primer and intermediate paint coats over the patch and apply final paint coat over entire unbroken surface containing the patch. Provide additional coats until patch blends with adjacent surfaces.

3.3.3.4. Ceilings: Patch, repair, or rehang in-place ceilings as necessary to provide an even-plane surface of uniform appearance.

3.3.3.5. Exterior Building Enclosure: Patch components in a manner that restores enclosure to a weather-tight condition.

3.3.3.6. Refinish surfaces to match adjacent finish. For continuous surfaces, refinish to nearest intersection or natural break. For an assembly, refinish entire unit.

3.3.3.7. At penetrations of fire rated walls, partitions, ceiling, or floor construction, completely seal voids with fire rated material to full thickness of the penetrated element.

3.3.3.8. Demolished Materials: Deliver to the Owner any material or parts that he wants for salvage. In particular, this includes all door hardware components replaced by this project.

3.3.4. Cleaning: Clean areas and spaces where cutting and patching are performed. Completely remove paint, mortar, oils, putty, and similar materials.

END OF SECTION
SECTION 01 75 00
STARTING AND ADJUSTING

1. PART 1 - GENERAL

1.1. SECTION INCLUDES

1.1.1. Starting systems.

1.1.2. Demonstration and instructions.

1.1.3. Testing and adjusting.

1.2. STARTING SYSTEMS

1.2.1. Coordinate schedule for start-up of various equipment and systems.

1.2.2. Notify Owner and Architect 48 hours prior to start-up of each item.

1.2.3. Verify that tests, meter readings, and specified electrical characteristics agree with those required by the equipment or system manufacturer.

1.2.4. Verify wiring and support components for equipment are complete and tested.

1.2.5. Execute start-up under supervision of responsible manufacturer's representative and/or Contractor personnel in accordance with manufacturers' instructions.

1.2.6. When specified in individual specification Sections, require manufacturer to provide authorized representative to be present at site to inspect, and check equipment or system installation prior to start-up and to supervise placing equipment or system operation.

1.2.7. Submit a written report to the Architect that equipment or system has been properly installed and is functioning correctly.

1.2.8. Provide advance notice to Architect and Inspector of Record regarding all coordination for utility and service systems hook-ups.

1.3. DEMONSTRATION AND INSTRUCTIONS

1.3.1. Demonstrate operation and maintenance of Products to Owner's personnel within seven (7) calendar days of Substantial Completion, prior to occupancy.

1.3.2. Demonstrate Project equipment by a qualified manufacturers' representative who is knowledgeable about the Project.

1.3.3. Utilize operation and maintenance manuals as basis for instruction. Review contents of manual with Owner's personnel in detail to explain all aspects of operation and maintenance.

1.3.4. Demonstrate start-up, operation, control, adjustment, trouble-shooting, servicing, maintenance and shutdown of each item of equipment at agreed-upon times at equipment location.
1.3.5. Prepare and insert additional data in operations and maintenance manuals when need for additional data becomes apparent during instruction.

2. **PART 2 - PRODUCTS**

   Not Used

3. **PART 3 - EXECUTION**

   Not Used

**END OF SECTION**
SECTION 01 77 19
CLOSEOUT REQUIREMENTS

1. PART 1 - GENERAL

1.1. SECTION INCLUDES

1.1.1. Closeout Procedures.

1.1.2. Final Cleaning.

1.1.3. Adjusting.

1.1.4. Project Record Documents.

1.1.5. Operation and Maintenance Data.

1.1.6. Warranties.

1.1.7. Spare Parts and Maintenance Materials.

1.2. SUBSTANTIAL COMPLETION AND PUNCH LIST PROCEDURES

1.2.1. At such time as the Contractor believes project is substantially complete, notify Architect Project Manager and request Punch List Inspection.

1.2.2. Architect and Architect’s Consultants will conduct an inspection in order to determine acceptance of work and identify items remaining to complete. The Architect will prepare a Punch List of such items and transmit to Contractor.

1.2.3. If Architect determines that punch list items remaining are sufficiently minor, and that Owner can occupy work and use it for its intended purpose, then Architect will prepare a Notice of Substantial Completion for Owner’s signature.

1.2.3.1. If work is not substantially complete, Contractor shall continue construction until such time as project status justifies subsequent inspection. Architect and Architect’s Consultant costs incurred in such subsequent inspections will be paid by Contractor by Owner-Contractor contract adjustment.

1.2.3.2. Contractor shall complete all items on Punch List within 30 days, or as stated on Notice of Substantial Completion.

1.3. FINAL COMPLETION PROCEDURES

1.3.1. At such time as Contractor believes project is complete and following completion of Punch List items, notify Architect and request Final Inspection

1.3.1.1. Submit written certification that Contract Documents have been reviewed, Work has been inspected, and that Work is complete in accordance with Contract Documents and ready for Architect Final inspection.

1.3.1.2. Upon receipt of request for final inspection, Architect will perform a Final Inspection and recommend actions as defined by the General Conditions.
1.3.1.3. If Architect determines work is acceptable under the Contract Documents, Contractor shall submit Final Application for Payment and close-out documents.

1.3.2. Final Application for Payment

1.3.2.1. Contractor shall submit final Application for Payment identifying total adjusted Contract Sum, previous payments, and sum remaining due.

1.3.2.2. Provide evidence of payment, lien releases and consent of surety to make final payment to Contractor.

1.3.2.3. Contractor shall provide all close-out documents required by Contract Documents within ten days of the last day of the contract period.

1.3.2.4. Close out documents include, but are not necessarily limited to:

1.3.2.4.1. Project Job Set and Record Set.

1.3.2.4.2. Operational and maintenance manuals and data.

1.3.2.4.3. Warranties and Guarantees.

1.3.2.4.4. Keys and keying schedules.

1.3.2.4.5. Spare parts, extra stock and materials.

1.3.2.4.6. All jurisdictional approval documents, including Final Verified reports, certification of fire alarm and related documents.

1.4. FINAL CLEANING

1.4.1. Contactor shall conduct all final cleaning required to comply with requirements of this Section prior to final inspection.

1.4.2. Use cleaning materials which do not create hazards to health or property and which will not damage surfaces. Use only those cleaning materials and methods recommended by manufacturer of the surface material to be cleaned. Use cleaning materials only on surfaces recommended by cleaning material manufacturer.

1.4.3. Employ experienced workers or professional cleaners for final cleaning. Comply with instructions of manufacturer for surface being cleaned.

1.4.4. Comply with regulations of authorities having jurisdiction and safety standards for cleaning. Do not burn waste materials. Do not bury debris or excess materials on the Owner’s property. Do not discharge volatile, harmful or dangerous materials into drainage systems. Remove waste materials from the site and dispose of in a lawful manner.

1.4.5. Contractor shall clean all completed interior work, including but not necessarily limited to, surfaces exposed to view in final construction, all cabinet/casework interiors and surfaces, and all equipment and fixtures.

1.4.5.1. Remove temporary labels, stains and foreign substances. Where stain cannot be removed, replace item to the satisfaction of the Project Manager and Architect.
1.4.5.2. Polish transparent and glossy surfaces.

1.4.5.3. Wet wipe painted and prefinished surfaces. Do not leave residue or wipe marks.

1.4.6. Remove waste and surplus materials, rubbish, and construction facilities from the site and legally dispose of.

1.5. ADJUSTING

1.5.1. Adjust operating Products and equipment to ensure smooth and unhindered operation.

1.6. RECORD DOCUMENTS: RECORD SET

1.6.1. Upon completion of the Work, obtain one set of reproducible drawings made from approved stamped originals from the Architect for preparation of Record Set. Cost to duplicate originals will be paid by Contractor at no further cost to Owner.

1.6.1.1. Neatly and accurately transfer data from record job set prints specified in Section 01 50 00.

1.6.1.2. Graphic quality shall be equal to that of the original document. Submit sample of drafting and graphic capability and obtain Architect’s approval before proceeding with transfer.

1.6.1.3. Cost of Record Set reproducibles and all preparation shall be paid by Contractor at no additional cost to Owner.

1.6.2. Sign and date Record Job Sets and Record Sets, certifying that the information and data added is accurate and complete.

1.6.3. Record drawings not complying with specified criteria shall be rejected.

1.6.4. Prior to submission for final payment, review Record Set with Architect and obtain approval of the scope of transfer. Following approval, submit Record Job Sets and Record Set to Architect with claim for final Application for Payment.

1.7. OPERATION AND MAINTENANCE DATA

1.7.1. Submit two sets prior to final inspection, bound in 8-1/2 x 11 inch text pages, three ring binders with durable plastic covers.

1.7.2. Prepare binder covers with printed title "OPERATION AND MAINTENANCE INSTRUCTIONS", title of project, and subject matter of binder when multiple binders are required.

1.7.3. Internally subdivide the binder contents with permanent page dividers, logically organized as described below; with tab titling clearly printed under reinforced laminated plastic tabs.

1.7.4. Contents: Prepare a Table of Contents for each volume, with each Product or system description identified, type on 24 pound white paper.

1.7.5. Part 1: Directory, listing names, addresses, and telephone numbers of Architect, Contractor, Subcontractors, and major equipment suppliers.
1.7.6. Part 2: Operation and maintenance instructions, arranged by system and subdivided by specification section. For each category, identify names, addresses, and telephone numbers of Subcontractors and suppliers. Identify the following:

1.7.6.1. Significant design criteria.
1.7.6.2. List of equipment.
1.7.6.3. Parts list for each component.
1.7.6.4. Operating instructions.
1.7.6.5. Maintenance instructions for equipment and systems.
1.7.6.6. Maintenance instructions for special finishes, including recommended cleaning methods and materials and special precautions identifying detrimental agents.

1.7.7. Part 3: Project documents and certificates, including the following:

1.7.7.1. Shop drawings and product data.
1.7.7.2. Certificates.
1.7.7.3. Photocopies of warranties.

1.7.8. Submit one copy of completed volumes in final form 15 days prior to final inspection. This copy will be returned after final inspection, with Architect comments. Revise content of documents as required prior to final submittal.

1.7.9. Submit final volumes revised, within 15 days after final inspection.

1.8. WARRANTIES

1.8.1. Provide duplicate notarized copies.
1.8.2. Execute and assemble documents from Subcontractors, suppliers, and manufacturers.
1.8.3. Provide Table of Contents and assemble in three ring binder with durable plastic cover.
1.8.4. Submit prior to final Application for Payment.
1.8.5. For items of Work delayed beyond date of Substantial Completion, provide updated submittal within ten days after acceptance, listing date of acceptance as start of warranty period.

1.9. SPARE PARTS AND MAINTENANCE MATERIALS

1.9.1. Provide products, spare parts, maintenance and extra materials in quantities specified in individual specification Sections.
1.9.2. Deliver to Project site and place in location as directed; obtain receipt prior to final payment.

2. PART 2 - PRODUCTS

Not used
3. PART 3 - EXECUTION

Not used

END OF SECTION
SECTION 08 71 00
DOOR HARDWARE

1. PART 1 – GENERAL

1.1. WORK INCLUDED

1.1.1. Door hardware.

1.1.2. Scope of Work in this Section: This section is provided to facilitate coordination with the hardware changes and modifications done for Proximity Card/Access equipment. The scope includes replacing any miscellaneous items damaged or removed during the work. Provide all finish hardware necessary to complete work.

1.2. WORK FURNISHED BUT INSTALLED UNDER OTHER SECTIONS

1.2.1. The contractor will deliver cylinder locks to PCC’s Lock Shop for re-keying and installation in new lever sets installed in this contract.

1.3. REFERENCES

1.3.1. Builders’ Hardware Manufacturers Association (BHMA) standards as specified.

1.3.2. Steel Door Institute (SDI) standards as specified.

1.3.3. Part 2, Title 24, CCR, 2007 edition, including all current amendments.

1.3.4. Americans with Disabilities Act Accessibility Guidelines (ADAAG) criteria as specified.

1.3.5. Underwriters Laboratories Inc. standards as specified.


1.4. QUALITY ASSURANCE

1.4.1. Hardware Supplier: Provide hardware that matches and is compatible with the existing door hardware. Supplier shall have in its employ a certified Architectural Hardware Consultant (AHC) to prepare submittals required by this Section and who shall be available at reasonable times, during the course of the work, for project hardware consultation to the Owner, Architect, and Contractor. In addition AHC shall certify hardware installation as specified in this Section.

1.4.2. Hardware supplier shall have a maintenance and service facility located within 100 miles of the project site. This facility will stock parts for products supplied and be capable of repairing and replacing hardware items found defective within the warranty period.

1.5. REGULATORY REQUIREMENTS

1.5.1. Hardware shall be tested and listed per UL10C. Furnish letter of compliance from each manufacturer in the submittals for each type of rated opening.

1.5.2. Conform to applicable requirements of the Americans with Disabilities Act Accessibility Guidelines regarding accessibility requirements for door and entrance hardware.
1.6. CERTIFICATIONS

1.6.1. Architectural Hardware Consultant provided by Contractor shall inspect preparation and initial installation of each type of hardware condition.

1.7. SUBMITTALS

1.7.1. Submit schedule and product data under provisions of Section 01 33 00.

1.7.2. Provide seven (7) copies of hardware schedule showing each application, the quantity required, part numbers and finish of each item.

1.7.2.1. Architects review of such schedule does not relieve the Contractor of providing all hardware required for the Work, whether or not such hardware was inadvertently omitted from Submittal. No extra cost will be allowed for changes or corrections necessary to facilitate the proper installation of hardware.

1.7.3. Accompanying schedules, provide two (2) manufacturer’s brochures of each item specified and scheduled, indicating function, finish, dimensions, and related features for electronic door and security hardware using computer processing. No hardware schedules will be accepted for review without submission of such brochure package.

1.7.4. Provide shop drawings showing all boxes, wiring and/or other support components of hardware assemblies enclosed or embedded in construction.

1.8. COORDINATION

1.8.1. Coordinate work of this Section with other directly affected Sections involving manufacturer of any internal reinforcement for door hardware.

1.8.1.1. In particular, coordinate door preparation/ modifications in accordance with applicable regulatory and trade standards specified.

1.8.2. Review all details and conditions prior to ordering hardware. If door hand is changed during construction, coordinate and change all hardware as necessary at no cost to the Owner.

1.9. OPERATION AND MAINTENANCE DATA

1.9.1. Submit operation and maintenance data under provisions of Section 01 77 19.

1.9.2. Include data on operating hardware, lubrication requirements, and inspection procedures related to preventative maintenance.

1.10. MAINTENANCE MATERIALS

1.10.1. Provide special wrenches and tools applicable to each different or special hardware component.

1.10.2. Provide maintenance tools and accessories supplied by hardware component manufacturer.
1.11.  WARRANTY AND GUARANTY

1.11.1.  Provide warranty from hardware supplier against all defects on all hardware, including electrical components, as follows:

1.11.1.1.  Card Reader assemblies, locksets and levers: Two years.
1.11.1.2.  Hinges: Life of the building.
1.11.1.3.  All other hardware: Two years.

1.11.2.  CONTRACTORS GUARANTEE

1.11.2.1.  Provide, in Architect approved form, the Owner with a guarantee against the following specific defects or failures for a period of three (3) years after Notice of Substantial Completion:

1.11.2.1.1.  Loose or misaligned components, resulting in the inability for the hardware assembly to function as intended or in compliance with applicable regulations.
1.11.2.1.2.  Finish failure, including rust, pitting, flaking and other finish appearance defects.

1.11.2.2.  Submit Guarantee on Manufacturer's form.

2.  PART 2 - PRODUCTS

2.1.  MANUFACTURERS

2.1.1.  Obtain each kind of hardware (latch and locksets, exit devices, hinges, and closers) to matching the existing hardware.

2.2.  DOOR HARDWARE CRITERIA

2.2.1.  Manufacturers:

2.2.1.1.  Hinges: Stanley (STA) to match existing and College Standards.
2.2.1.2.  Locks and Latch sets: ASSA "Sierra" (SR) design.

2.2.1.2.1.  Finish to be: US 26D, BHMA-626, satin chrome.
2.2.1.2.2.  Lockset backset to be two and three-quarter inches (2.75").
All dimensions must conform to the American National Standards Institute (ANSI) specifications.

2.2.1.3.  Cylinders are existing key-in knob, removed from existing doors undergoing change to card access. Deliver these to the Pima College Lock Shop for re-keying and re-installation into the new lever latches installed in this contract.
2.2.2. Finishes

2.2.2.1. Finishes are to match the existing.

2.2.2.2. Provide black colored seals unless specified otherwise.

2.2.2.3. Provide fasteners matching in finish, base material and color.

2.2.2.4. Where door has a fire resistance rating, provide UL Listed and labeled hardware.

2.2.3. Contractor and hardware supplier shall meet with the Owners Representative and Architect to review the existing conditions of each door.

2.2.3.1. Photograph each door prior to starting work to document the condition.

2.2.3.2. Review any issues regarding the installation of new locksets.

2.2.3.3. Provide the salvaged locksets and cylinders to Pima Community College.

2.2.3.4. Establish an acceptable time frame to allow the PCC lock shop to rekey the cylinders and reinstall them.

2.2.3.5. Owner's representative: Michael Posey, phone (520) 206-2661.

2.3. OTHER MATERIALS

2.3.1. Provide all other materials, not specifically described but required for complete and proper installation of this work, as selected by the contractor and subject to the approval of the Architect.

3. PART 3 - EXECUTION

3.1. SURFACE CONDITIONS

3.1.1. Inspection

3.1.1.1. Prior to all work of this section, carefully inspect the installed work of all other trades and verify that all such work is complete to the point where this installation may properly commence.

3.1.1.2. Verify that work of this Section may be installed in strict accordance with the original design, all pertinent codes and regulations, and all pertinent portions of the referenced standards.

3.1.1.2.1. Verify that power supply of proper voltage and type is available to power operated devices.

3.1.1.3. In the event of discrepancy, immediately notify the Architect.

3.1.1.4. Do not proceed with installation in areas of discrepancy until all such discrepancies have been fully resolved.
3.2. INSTALLATION

3.2.1. Install hardware in accordance with manufacturer’s instructions and requirements of SDI, ANSI/NFPA 80, AWS, and BHMA. Select applicable standard based on door function, type and regulatory criteria.

3.2.1.1. On fire labeled doors, do not field machine any door assemblies.

3.2.1.2. Install hardware in accordance with NFPA 80, the manufacturers listing requirements and UL 10C for positive pressure labeling requirements on fire labeled doors.

END OF SECTION
SECTION 260500
COMMON WORK RESULTS FOR ELECTRICAL

PART 1 - GENERAL

1.1 RELATED DOCUMENTS
A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY
A. Section Includes:
   1. Electrical equipment coordination and installation.
   2. Common electrical installation requirements.

1.3 COORDINATION
A. Coordinate arrangement, mounting, and support of electrical equipment:
   1. To allow maximum possible headroom unless specific mounting heights that reduce headroom are indicated.
   2. To provide for ease of disconnecting the equipment with minimum interference to other installations.
   3. To allow right of way for piping and conduit installed at required slope.
   4. So connecting raceways, cables, wireways, cable trays, and busways will be clear of obstructions and of the working and access space of other equipment.

B. Coordinate installation of required supporting devices as they are constructed.
C. Coordinate location of access panels and doors for electrical items that are behind finished surfaces or otherwise concealed.
D. Coordinate sleeve selection and application with selection and application of firestopping.

PART 2 - EXECUTION

2.1 COMMON REQUIREMENTS FOR ELECTRICAL 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 electrical 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.

2.2 FIRESTOPPING

A. Apply firestopping to penetrations of fire-rated floor and wall assemblies for electrical installations to restore original fire-resistance rating of assembly.

END OF SECTION
SECTION 260519

LOW-VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. This Section includes the following:

1. Building wires and cables rated 600 V and less.
2. Connectors, splices, and terminations rated 600 V and less.

B. Codes and Standards. All materials provided under the Section shall conform to:

1. American Society for Testing and Materials (ASTM): Comply with requirements of the following:
   a. B3 Standard Specification for Soft or Annealed Copper Wire
   b. B 8 Standard Specification for Concentric-Lay-Stranded Copper Conductors, Hard, Medium-Hard, or Soft
   c. D 753 Standard Specification for General Purpose Polychloroprene Jacket for Wire and Cable

2. Electrical Testing Laboratories (ETL): Provide wiring, cabling and connector products which are ETL listed and labeled.

3. Institute of Electrical and Electronics Engineers (IEEE): Comply with the following standards which apply to wiring systems:
   a. 82 Test Procedure for Impulse Voltage Tests on Insulated Conductors
   b. 241 Recommended Practice for Electric Power Systems in Commercial Buildings

4. NFPA: Comply with NFPA 70 requirements for construction, installation and color coding of electrical wire, cable and connections.

5. National Electrical Manufacturers Association (NEMA): Comply with requirements of the following:
   a. WC 3 Rubber-Insulated Wire and Cable for the Transmission and Distribution of Electrical Energy
   b. WC 5 Thermoplastic-Insulated Wire and Cable for the Transmission and Distribution of Electrical Energy
   c. WC 7 Cross-Linked-Thermosetting-Polyethylene-Insulated Wire and Cable for the Transmission and Distribution of Electrical Energy

6. UL: Provide wiring, cabling and connector products which are UL listed and labeled in conformance with the following standards:
   a. 4 Armored Cable
   b. 44 Rubber-Insulated Wires and Cables
   c. 83 Thermoplastic-Insulated Wires and Cables
   d. 486A Wire Connectors and Soldering Lugs for Use with Copper Conductors
   e. 854 Service-Entrance Cables
1.3 SUBMITTALS
A. Product Data: Submit manufacturer's data on electrical wire, cables, conductors, connectors and connector crimping tools where specified.

1.4 DELIVERY, STORAGE AND HANDLING
A. Delivery: Deliver wire and cable packaged in factory sealed containers, or wound on NEMA wire and cable reels.
B. Storage: Store wire and cable in a clean dry space in original containers. Protect products from weather, damaging fumes, construction debris and traffic.
C. Handling: Handle wire and cable carefully to avoid abrading, puncturing and tearing wire and cable insulation and sheathing. Ensure that dielectric resistance integrity of wires/cables is maintained.

1.5 QUALITY ASSURANCE
A. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.
B. Comply with NFPA 70.

PART 2 - PRODUCTS
2.1 CONDUCTORS AND CABLES
A. Available Manufacturers: Subject to compliance with requirements, manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:
   2. General Cable Corporation.
B. Copper Conductors: Comply with NEMA WC 70.
   1. Provide wire rated 600 V minimum of the stranded conductor annealed copper type.
      a. Conductors No. 12 AWG and smaller
      b. Conductivity shall not be less than 98 percent at 20 degrees C. (68 degrees F.) or resistivity greater than 1.7 microhms per centimeter.
      c. For branch circuit wiring use a minimum wire size of No. 12.
   c. Conductor Insulation: Comply with NEMA WC 70.
      1. Provide the following types of insulation.
         a. For dry locations with copper conductors, provide Type THHN/THWN, or XHHW.
         b. For wet locations provide Type XHHW-2.
   d. Cable:
1. Provide UL listed cables of sizes, ampacity temperature ratings and insulating materials indicated on the drawings.

E. Prohibited products:

1. The use of non-metallic sheathed cable Types NM to NMC, armored-bushed cable (BX), armor-clad cable (AC) and metal clad cable (MC) is prohibited.

2.2 CONNECTORS AND SPLICES

A. Available Manufacturers: Subject to compliance with requirements, manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. AFC Cable Systems, Inc.
3. O-Z/Gedney; EGS Electrical Group LLC.
4. 3M; Electrical Products Division.

B. General: Provide UL listed metal connectors of sizes, ampacity, temperature ratings, materials, and classes required by NFPA 70 and NEMA standards for applications and services indicated.

C. Connectors:

1. For wires No. 10 AWG and smaller, provide solderless, insulated pressure cable type connectors, 600 V, of the compression or indent type or wire nut connectors. Temperature rating of connectors shall be at least equal to that of the wire on which they are used.

2.3 INSULATING TAPE, PUTTY, RESIN AND SUPPORTS

A. Tape: Provide plastic electrical insulating tape which is flame retardant, cold and weather resistant. Tape for use in areas subject to temperatures 30 degrees C. to 105 degrees C., or where the tape will be subjected to an oil splash, tape shall have a minimum thickness of 8.5 mils, and shall consist of an oil-resistant vinyl backing with an oil-resistant acrylic adhesive.

B. Materials: Provide all insulating materials for splices and connections such as glass and synthetic tapes, putties, resins, splice cases, or compositions of the type approved for the particular use, location, voltage and temperature, and apply and install in an approved manner, all in accordance with the manufacturer's recommendations.

PART 3 - EXECUTION

3.1 CONDUCTOR MATERIAL APPLICATIONS

A. Branch Circuits: Copper. stranded.

3.2 CONDUCTOR INSULATION AND MULTICONDUCTOR CABLE APPLICATIONS AND WIRING METHODS

A. Exposed Branch Circuits, Including in Crawlspace: Type THHN-THWN, single conductors in raceway.
B. Branch Circuits Concealed in Ceilings, Walls, and Partitions: Type THHN-THWN, single conductors in raceway.

C. Branch Circuits Concealed in Concrete, below Slabs-on-Grade, and Underground: Type XHHW, single conductors in raceway.

D. Cord Drops and Portable Appliance Connections: Type SO, hard service cord with stainless-steel, wire-mesh, strain relief device at terminations to suit application.

E. Class 1 Control Circuits: Type THHN-THWN, in raceway.

F. Class 2 Control Circuits: Type THHN-THWN, in raceway.

3.3 INSTALLATION OF CONDUCTORS AND CABLES

A. General: Install electrical wires, cables and wiring connectors in compliance with applicable requirements of NFPA 70, NEMA, UL and National Electrical Contractors Association (NECA) "Standard of Installation."

B. Conduit: Unless otherwise noted, install all wiring in rigid metal conduit, electric metallic tubing, flexible metal conduit, and non-metallic conduit as indicated on the drawings, in conformance with NFPA 70.

1. Conceal cables in finished walls, ceilings, and floors, unless otherwise indicated.

C. Complete System: Provide wire, cables and connectors necessary for a complete installation from point of service connection to all receptacles, lighting fixtures, devices, utilization equipment and outlets for future extensions as indicated on the drawings, in schedules, and in the specification. Provide ample slack wire for connections.

1. Use manufacturer-approved pulling compound or lubricant where necessary; compound used must not deteriorate conductor or insulation. Do not exceed manufacturer's recommended maximum pulling tensions and sidewall pressure values.

2. Use pulling means, including fish tape, cable, rope, and basket-weave wire/cable grips, that will not damage cables or raceway. Provide suitable installation equipment to prevent cutting and abrasion of conduits during the pulling of wires and cables.

3. Install exposed cables parallel and perpendicular to surfaces of exposed structural members, and follow surface contours where possible.

4. Support cables according to Division 26 Section "Hangers and Supports for Electrical Systems."

D. Voltage Rating: Wire and cables for general wiring shall be rated for 600 volts minimum. Where the operating voltage is less than 100 V, wire and cables may be insulated for 300 V, provided they are completely isolated from other higher voltage systems.

E. Minimum Size: Minimum branch circuit conductor size shall be No. 12 AWG. Said conductor sizes shall be used for full length of circuit, unless noted otherwise.

F. Shelf Life: Wire and cable manufactured more than 12 months prior to date of delivery to the site shall not be used.

G. Bundling: Neatly and securely bundle all conductors located in branch circuit panelboards, pullboxes, signal cabinets, signal control boards, switchboards and motor control centers. Bundle and cable with nylon straps made of self-extinguishing nylon having a temperature...
range of -65 degrees F. to +350 degrees F. Each strap shall be constructed with a locking hub or head on one end and a taper on the other.

3.4 CONNECTIONS

A. Tighten electrical connectors and terminals (including screws and bolts) according to manufacturer's published torque-tightening values. If manufacturer's torque values are not indicated, use those specified in UL 486A and UL 486B.

B. Make splices and taps that are compatible with conductor material and that possess equivalent or better mechanical strength and insulation ratings than unspliced conductors.

1. Keep conductor splices to a minimum. Splice wires and cables only in outlet boxes, junction boxes, pullboxes and handholes.
2. In the making of a splice, connectors shall be brought up securely upon the conductors such that all conductors are equally engaged, the insulation is not ruptured, no bare wires are exposed or have "backed off" due to the application of pressure and the connection will not loosen due to cycling or vibration, in order to insure an efficient splice.
3. The number, size and combinations of conductors permitted as listed on manufacturer's packaging of connector shall be strictly followed.
4. Connectors shall be fully insulated by a skirt, or taped to provide an insulation value at least equal to rating of wires being connected.

C. Connectors: Tighten electrical connectors and terminals, including screws and bolts, in accordance with manufacturer's published torque tightening values or comply with tightening torques specified in UL 486A and 486B.

D. Wiring at Outlets: Install conductor at each outlet, with at least 6 inches (150 mm) of slack.

3.5 COLOR CODING

A. Color code all secondary service, feeder and branch circuit conductors throughout the project secondary electrical system as follows:

1. 208Y/120Volts  Phase  480Y/277 Volts

<table>
<thead>
<tr>
<th>Color</th>
<th>Code</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black</td>
<td>A</td>
<td>Brown</td>
</tr>
<tr>
<td>Red</td>
<td>B</td>
<td>Orange</td>
</tr>
<tr>
<td>Blue</td>
<td>C</td>
<td>Yellow</td>
</tr>
<tr>
<td>White</td>
<td>Neutral</td>
<td>Gray</td>
</tr>
<tr>
<td>Green</td>
<td>Ground</td>
<td>Green</td>
</tr>
<tr>
<td>Green with</td>
<td>Isolated Ground</td>
<td>--</td>
</tr>
<tr>
<td>Yellow Strip</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. The colors shall be factory-applied entire length of the conductors by one of the following methods except as noted and limited below:
   a. Solid color compound.
   b. Solid color coating.
   c. Surface printing every 12 inches, maximum spacing of 18 inches.
3. All branch circuit conductors Nos. 12 AWG and 10 AWG shall be solid color compound or solid color coating.
4. All sizes of conductors used for equipment grounds No. 6 AWG and smaller shall be solid compound or solid color coating green.
5. All phase conductors No. 8 AWG and larger color-coded with pressure sensitive tape shall have a background color other than white or green.
6. Field applied color coding methods may be used in lieu of factory coded wire in sizes larger than N. 10 AWG for phase and neutral conductors.
7. Color pressure-sensitive plastic tape shall be applied in half overlapping turns for a distance of six inches or all terminal points and in all boxes in which splices or taps are made. The last two laps of tape shall be applied with no tension to prevent possible unwinding.

3.6 FIRESTOPPING
A. Apply firestopping to electrical penetrations of fire-rated floor and wall assemblies to restore original fire-resistance rating of assembly.

3.7 INSTALLATION IN PULLBOXES
A. Support: Install and support cables in pullboxes. Train cable but do not bend cable to radius equal to less than six times overall cable diameter.
B. Splices: Do not make splices in underground systems in accessible locations such as pullboxes and handholes, unless indicated otherwise. Conductors shall be looped and pulled through all pullboxes and handholes.

3.8 FIELD QUALITY CONTROL
A. Perform tests and inspections and prepare test reports.
B. Tests and Inspections:
   1. After installing conductors and cables and before electrical circuitry has been energized, test conductors for compliance with requirements.
C. Test Reports: Prepare a written report to record the following:
   1. Test procedures used.
   2. Test results that comply with requirements.
   3. Test results that do not comply with requirements and corrective action taken to achieve compliance with requirements.
D. Remove and replace malfunctioning units and retest as specified above.

END OF SECTION 260519
SECTION 260526
GROUNDING AND BONDING FOR ELECTRICAL SYSTEMS

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. This Section includes methods and materials for grounding systems and equipment specified on project documents. The solid grounding specified in this Section shall be applied to the grounding of the following:
   1. Electrical equipment enclosures.
   2. Electrically operated equipment.

B. Codes and Standards. All materials and work specified in this section shall conform to the following standards:
   1. American National Standards Institute (ANSI): Comply with the requirements of:
   2. American Society for Testing and Materials (ASTM): Comply with the requirements of:
      a. Standard Specification for Hard-Drawn Copper Wire
      c. B 3 Standard Specification for Soft or Annealed Copper Wire
      e. B 228 Standard Specification for Concentric-Lay-Stranded Copper-Clad Steel Conductors.
   3. Institute of Electrical and Electronics Engineers (IEEE): Comply with the following standards which apply to the grounding of electrical systems:
      a. 141Recommended Practice for Electric Power Distribution for Industrial Plants.
      b. 142Recommended Practice for Grounding of Industrial and Commercial Power Systems.
   4. National Fire Protection Association (NFPA): Comply with the requirements of NFPA 70, “National Electrical Code” for the grounding of electrical systems. All devices and components provided under this section shall be listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.
   5. Underwriters Laboratories, Inc. (UL): Provide material and installation conforming to the following standards:
1.3 SUBMITTALS

A. Product Data: For each type of product indicated, submit manufacturer’s data on conductors, grounding electrodes, ground clamps, and exothermic welding devices where specified.

B. Qualification Data: For testing agency and testing agency’s field supervisor.

C. Field quality-control test reports.

PART 2 - PRODUCTS

2.1 MANUFACTURERS

A. Available Manufacturers: Subject to compliance with requirements, manufacturer’s offering products that may be incorporated into the Work include, but are not limited to:
   1. Southwire.
   2. Rome.
   3. Essex.
   5. Capital.

2.2 GENERAL GROUNDING SYSTEM REQUIREMENTS

A. Materials: Provide an electrical system and equipment grounding system consisting of an assembly of materials including, but not limited to, cables, connectors, ground rods, bonding jumpers, surge arresters, and all accessories necessary to make a complete installation. All materials utilized in the grounding system shall meet the requirements of the standards listed and shall also meet established industry standards for the applications indicated.

B. Components: Provide raceways, boxes and fittings for grounding conductors. Install grounding conductors in one or more of the following types of raceway unless direct buried or exposed conductors are specified:
   1. Galvanized rigid steel conduit
   2. Electric metallic tubing (EMT)
   3. Flexible steel conduit
   4. Liquid tight flexible steel conduit
   5. PVC conduit

C. Where grounding conductors are routed in ferrous conduit, each end of said conduit shall be bonded to ground.

2.3 CONDUCTORS

A. Insulated Conductors: Provide green insulated equipment grounding conductors which run in the same raceway with circuit wires for all electrical and fire alarm conduits. Copper or tinned-
copper wire or cable insulated for 600 V unless otherwise required by applicable Code or authorities having jurisdiction.

B. Bare Copper Conductors: Provide bare ground conductors for grounding of transformers, switchgear, other service equipment, grounding service poles and electrical equipment structures both underground and above ground. Conductors shall be stranded copper conductors.

4. Sizes and types of conductors in four subparagraphs below are typical examples. 28-kcmil bonding cable in first subparagraph below is slightly larger than No. 6 AWG.
5. Bonding Cable: 28 kcmil, 14 strands of No. 17 AWG conductor, ¼ inch (6 mm) in diameter.
6. Bonding Conductor: No. 4 or No. 6 AWG, stranded conductor.
7. Bonding Jumper: Provide braided copper tape constructed of No. 30 gauge bare copper wires sized to suit the application. Copper tape, braided conductors, terminated with copper ferrules; 1-5/8 inches (41 mm) wide and 1/16 inch (1.6 mm) thick.
8. Tinned Bonding Jumper: Tinned-copper tape, braided conductors, terminated with copper ferrules; 1-5/8 inches (41 mm) wide and 1/16 inch (1.6 mm) thick.

C. Grounding Bus: Rectangular bars of annealed copper, ¼ by 2 inches (6 by 50 mm) in cross section, unless otherwise indicated; with insulators.

2.4 CONNECTORS

A. Listed and labeled by a nationally recognized testing laboratory acceptable to authorities having jurisdiction for applications in which used, and for specific types, sizes, and combinations of conductors and other items connected.

B. Bolted Connectors for Conductors and Pipes: Copper or copper alloy, bolted pressure-type, with at least two bolts.

1. Pipe Connectors: Clamp type, sized for pipe.

C. Welded Connectors: Exothermic-welding kits of types recommended by kit manufacturer for materials being joined and installation conditions.

2.5 GROUNDING ELECTRODES

A. Ground Rods: Copper-clad steel; ¾ inch by10 feet (19 mm by 3 m) in diameter.

B. Multiple Ground Rods: Where the grounding resistance specified on the drawings can not be achieved with a single rod, provide multiple ground rods as necessary to achieve the level of ground resistance required.

C. Ground Rod Identification: On each ground rod provided, the manufacturer shall die stamp, near the top, his name or trademark and the length of the rod in feet. All rods shall have a hard, clean, smooth continuous surface throughout the entire length of the rod.
2.6 SURGE SUPPRESSION

A. General: Where indicated, provide single- or three-phase surge arresters having voltage rating compatible with the circuit on which they are applied.

2.7 FIELD WELDING

A. General: Where welded connections are indicated or required, such as buried connections to cables or ground rods, such welds shall be made by the exothermic process utilizing factory provided molds.

PART 3 - EXECUTION

3.1 APPLICATIONS

A. Conductors: Install solid conductor for No. 8 AWG and smaller, and stranded conductors for No. 6 AWG and larger, unless otherwise indicated.

3.2 EQUIPMENT GROUNDING

A. Install insulated equipment grounding conductors with all feeders and branch circuits. Size all required equipment grounding conductors and strops in compliance with NFPA 70. Provide green colored insulation on all equipment grounding conductors of the same type and class as that specified for the associated phase and neutral conductors of the secondary distribution system. Braze or connect the feeder and branch circuit grounding conductors to the ground bus with approved pressure connectors.

B. Install insulated equipment grounding conductors with the following items, in addition to those required by NFPA 70:

1. Feeders and branch circuits. Provide a separate green insulated equipment grounding conductor for each single or three phase feeder and each branch circuit with a three phase protective device. Install the required grounding conductor in the common conduit with the related phase and neutral conductors. Where parallel feeders are installed in more than one raceway, provide a green insulated equipment grounding conductor in each raceway.

2. Receptacle circuits. Provide single phase branch circuits for 120 volt receptacle circuits consisting of phase neutral and green unshielded equipment grounding conductor installed in a common conduit.

3. Flexible raceway runs. Provide flexible steel conduit equipment connections utilized in conjunction with single phase branch circuits with green insulated grounding conductors connected to suitable grounding terminals at each end of the flexible conduit.

C. Signal and Communication Equipment: For telephone, alarm, voice and data, and other communication equipment, provide No. 12 AWG minimum insulated grounding conductor in raceway.

1. Terminal Cabinets: Terminate grounding conductor on cabinet grounding terminal.

3.3 BRANCH CIRCUIT GROUNDING REQUIREMENTS

A. General: Provide, in the same raceway with the associated phase and neutral conductors, a green colored equipment ground conductor having the same type and class insulation as the associated branch circuit conductors. Provide each ground conductor with spade type terminals or solderless pressure connectors to suit the requirements of the circuit.

B. Branch Circuit Ground Conductors: Connect ground conductors for branch circuits as follows:

1. Connect the ground conductor, accompanying the circuit serving the receptacle, to a green No. 10-32 “washer-in-head” machine screw threaded to the receptacle outlet box. Extend a green insulated ground wire from the ground terminal on the receptacle to this ground screw. Receptacles with special cast boxes having factory designed and approved ground paths shall require a separate ground jumper.

2. Provide an insulated ground wire from the green No. 10-32 machine screw in each ceiling outlet box or above ceiling junction box through the stem or flexible conduit to the ground terminal on each luminaire.

3. Provide an insulated ground wire from the ground terminal in the associated junction box or disconnect enclosure to a motor through the flexible conduit connection.

3.4 INSTALLATION

A. Grounding Conductors: Route along shortest and straightest paths possible, unless otherwise indicated or required by Code. Avoid obstructing access or placing conductors where they may be subjected to strain, impact, or damage.

3.8 FIELD QUALITY CONTROL

A. Perform the following tests and inspections and prepare test reports:

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

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

1. See Evaluations for discussion on appropriate ground resistance values. Listed below are typical maximum permitted values for different grounding applications; retain and edit applicable subparagraphs. Coordinate with requirements in Sections specifying equipment to be grounded.

2. Power and Lighting Equipment or System with Capacity 500 kVA and Less: 10 ohms.

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

END OF SECTION 260526
SECTION 260529
HANGERS AND SUPPORTS FOR ELECTRICAL SYSTEMS

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. This Section includes the following:

1. Hangers and supports for electrical equipment and systems.

1.3 DEFINITIONS

A. EMT: Electrical metallic tubing.

1.4 PERFORMANCE REQUIREMENTS

A. Design supports for multiple raceways capable of supporting combined weight of supported systems and its contents.

1.5 SUBMITTALS

A. Product Data: For the following:

1. Steel slotted support systems.

1.6 QUALITY ASSURANCE

A. Comply with NFPA 70.

PART 2 - PRODUCTS

2.1 SUPPORT, ANCHORAGE, AND ATTACHMENT COMPONENTS

A. Steel Slotted Support Systems: Comply with MFMA-4, factory-fabricated components for field assembly.

1. Available Manufacturers: Subject to compliance with requirements, manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:
a. Allied Tube & Conduit.
b. Cooper B-Line, Inc.; a division of Cooper Industries.
c. ERICO International Corporation.
d. GS Metals Corp.
e. Thomas & Betts Corporation.
f. Unistrut; Tyco International, Ltd.
g. Wesanco, Inc.

B. Raceway and Cable Supports: As described in NECA 1 and NECA 101.

C. Conduit and Cable Support Devices: Steel hangers, clamps, and associated fittings, designed for types and sizes of raceway or cable to be supported.

D. Support for Conductors in Vertical Conduit: Factory-fabricated assembly consisting of threaded body and insulating wedging plug or plugs for non-armored electrical conductors or cables in riser conduits. Plugs shall have number, size, and shape of conductor gripping pieces as required to suit individual conductors or cables supported. Body shall be malleable iron.

PART 3 - EXECUTION

3.1 APPLICATION

A. Comply with NECA 1 and NECA 101 for application of hangers and supports for electrical equipment and systems except if requirements in this Section are stricter.

B. Maximum Support Spacing and Minimum Hanger Rod Size for Raceway: Space supports for EMT, IMC, and RMC as required by NFPA 70. Minimum rod size shall be 1/4 inch (6 mm) in diameter.

C. Multiple Raceways or Cables: Install trapeze-type supports fabricated with steel slotted support system, sized so capacity can be increased by at least 25 percent in future without exceeding specified design load limits.
   1. Secure raceways and cables to these supports with two-bolt conduit clamps.

D. Spring-steel clamps designed for supporting single conduits without bolts may be used for 1-1/2-inch (38-mm) and smaller raceways serving branch circuits and communication systems above suspended ceilings and for fastening raceways to trapeze supports.

3.2 SUPPORT INSTALLATION

A. Comply with NECA 1 and NECA 101 for installation requirements except as specified in this Article.

B. Raceway Support Methods: In addition to methods described in NECA 1, EMT, IMC, and RMC may be supported by openings through structure members, as permitted in NFPA 70.

C. Strength of Support Assemblies: Where not indicated, select sizes of components so strength will be adequate to carry present and future static loads within specified loading limits. Minimum static design load used for strength determination shall be weight of supported components plus 200 lb (90 kg).
D. Mounting and Anchorage of Surface-Mounted Equipment and Components: Anchor and fasten electrical items and their supports to building structural elements by the following methods unless otherwise indicated by code:

1. To Wood: Fasten with lag screws or through bolts.
2. To New Concrete: Bolt to concrete inserts.
3. To Masonry: Approved toggle-type bolts on hollow masonry units and expansion anchor fasteners on solid masonry units.
4. To Existing Concrete: Expansion anchor fasteners.
5. To Steel: Beam clamps (MSS Type 19, 21, 23, 25, or 27) complying with MSS SP-69
6. To Light Steel: Sheet metal screws.
7. Items Mounted on Hollow Walls and Nonstructural Building Surfaces: Mount cabinets, panelboards, disconnect switches, control enclosures, pull and junction boxes, transformers, and other devices on slotted-channel racks attached to substrate.

E. Drill holes for expansion anchors in concrete at locations and to depths that avoid reinforcing bars.

END OF SECTION 260529
PART 1 - GENERAL

1.1 RELATED DOCUMENTS
A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY
A. This Section includes raceways, fittings, boxes, enclosures, and cabinets for electrical wiring.

1. Types of raceways in this Section include the following:
   a. Electrical metallic tubing.
   b. Flexible steel conduit.
   c. Surface metal raceways.
   d. Wireway.

2. Types of electrical boxes and fittings in this Section include the following:
   a. Outlet boxes
   b. Junction boxes
   c. Conduit bodies
   d. Bushings
   e. Locknuts
   f. Knockout closures

3. Types of electrical enclosures and cabinets in this Section include the following:
   a. Hinged Cover Enclosures

B. Codes and Standards: Conform to the Following:

1. American National Standards Institute (ANSI):
   a. C80.2 Rigid and Steel Conduit
   b. C80.3 Electrical Metallic Tugin – Zinc Coated
   c. 870 Wireways, Auxiliary Gutters and Associated Fittings

2. National Electrical Manufacturers Association (NEMA):
   a. FB1 Fittings, Cast Metal Boxes, and Conduit Boxes for Conduit and Cable assemblies.
   b. OS 1 Sheet-Steel Outlet Boxes, Device Boxes, Covers and Box Supports
   c. TC2 Electrical Plastic Tubing (EPT) and Conduit (EPC-80)
   d. TC3 PVC Fittings for Use With Rigid PVC Conduit and Tubing
   e. TC6 PVC and ABS Plastic Utilities Duct for Underground Installation

3. National Fire Protection Association (NFPA): Conform to the requirements of NFPA 70, “National Electrical Code” for application, size, location and installation of each type of raceway used. All Equipment specified in this section shall be listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.
4. Underwriters Laboratories, Inc. (UL): Provide raceways, electrical boxes and fittings which are UL-listed and labeled and conform to the following:
   a. UL 1 Flexible Metal Conduit
   b. UL 5 Surface Metal Raceways and Fittings
   c. UL 50 Cabinets and Boxes
   d. UL 360 Liquid-Tight Flexible Conduit
   e. UL 514A Metallic Outlet Boxes
   f. UL 514B Fittings for Conduit and Outlet Boxes

1.3 DEFINITIONS
   A. EMT: Electrical metallic tubing.
   B. FMC: Flexible metal conduit.
   C. IMC: Intermediate metal conduit.
   D. LFMC: Liquidtight flexible metal conduit.

1.4 SUBMITTALS
   A. Product Data:
      1. For raceways, submit manufacturer's data for items listed, including specifications, installation instructions and general recommendations.
         a. Surface metal raceway.
         b. Wireway.
         c. Flexible steel and liquid tight steel conduit and fittings.
         d. Metallic conduits and fittings.
      2. For cabinets and enclosures: Submit manufacturer's data on electrical cabinets and enclosures.
   B. Shop Drawings: Include plans, elevations, sections, details, and attachments to other work.
      1. Submit dimensioned drawings of electrical cabinets and enclosures

PART 2 - PRODUCTS

2.1 METAL CONDUIT AND TUBING
   A. Available Manufacturers: Subject to compliance with requirements, manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:
      1. AFC Cable Systems, Inc.
      2. Alflex Inc.
      3. Allied Tube & Conduit; a Tyco International Ltd. Co.
      4. Anamet Electrical, Inc.; Anaconda Metal Hose.
      5. Electri-Flex Co.
      7. Maverick Tube Corporation.
   B. Metal Conduit and Tubing: Provide conduit and tubing in conformance with the following:
      1. Minimum Size: Provide not less than 3/4-inch trade size.
         a. Size conduit and raceway in accordance with NFPA 70 unless otherwise specified or shown on the drawings.
3. Communications Conduits: Provide not less than 3/4-inch trade size.

4. Equipment Ground Conductor (Green): Raceway sizes shall be adequate to include the circuit conductors, an equipment ground conductor and a neutral conductor in accordance with percentage of fill requirements by NFPA 70. Size all conduits supplying motors and associated control equipment to include grounding conductor sized per NFPA 70.
   a. All junction boxes shall be in accordance with NFPA 70 as to conductor capacity for the future conductors with adequate knockouts on all four sides and a blank screw fastened cover. Provide a pull-wire in all empty conduits.

5. Electrical Metallic Tubing (EMT):
   b. Do not bury in ground or in slabs on grade.
   c. Do not use in concrete decks.
   d. Do not install exposed where subject to physical damage. Do not use less than 10 feet above grade at exterior locations.
   e. May be used in masonry walls and grouted cells.
   f. May be used in all interior locations not subject to physical damage.

6. Flexible Steel Electrical Conduit:
   a. Use in dry location.
   b. Do not use in corrosive atmosphere or exterior locations.
   c. Use only to connect recessed ceiling mounted light fixtures or smoke detectors.
   d. Use where conduit must be fished in building voids or in millwork.

C. Raceway Fittings, Couplings and Connectors:
   1. Use fittings listed and approved for specific conduit or raceway system used; e.g.: Use EMT fittings with EMT conduit.
   2. For threaded rigid steel conduit do not use threadless, set screw, or compression type fittings. Provide one piece threaded couplings and lock nuts.
   3. For EMT, provide steel couplings and connectors, compression, locking type with insulated throat. Do not use indentation type of fitting.
   4. Bushings shall be insulated type which also maintain continuity of conduit grounding system. Insulating material shall be molded or locked into metallic body of the fitting. Bushing made entirely of nonmetallic material will not be allowed.
   5. Provide flexible metal conduit fittings made of steel or malleable iron. They shall be insulated and one of the following types:
      a. Wedge and screw type having an angular wedge fitting between the convolutions of the conduit.
      b. Squeeze or clamp type having a bearing surface contoured to wrap around the conduit and clamped by one or more screws.
      c. Steel, multiple point type, for threading into internal wall of the conduit convolutions.
   6. All locknuts shall be the bonding type with sharp edges for digging into the metal wall of an enclosure.

2.2 METAL WIREWAYS AND RACEWAYS

A. Available Manufacturers: Subject to compliance with requirements, manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:
1. Cooper B-Line, Inc.
2. Hoffman.
3. Square D; Schneider Electric.
4. Wiremold.

B. Description: Sheet metal sized and shaped as indicated, unless otherwise indicated.

C. Fittings and Accessories: Include couplings, offsets, elbows, expansion joints, adapters, hold-down straps, end caps, and other fittings to match and mate with wireways as required for complete system.

D. Wireway Covers: Hinged type unless otherwise indicated.

E. Finish: As Indicated.

F. Wireways, Auxiliary Gutters:

1. May be used to facilitate installation and future changes in wiring between panelboards, safety switches in close proximity to each other on same or adjacent walls or in same electrical equipment room or area.
2. Provide weatherproof enclosure where outdoors or subject to moisture and similar elements.
3. Use where shown on drawings or specified.
4. Shall be completely accessible and identified per Division 16 specifications.

2.3 BOXES, ENCLOSURES, AND CABINETS

A. Available Manufacturers: Subject to compliance with requirements, manufacturers offering products that may be incorporated into the Work include, but are not limited to, the following:

1. Cooper Crouse-Hinds; Div. of Cooper Industries, Inc.
2. EGS/Appleton Electric.
7. RACO; a Hubbell Company.
10. Spring City Electrical Manufacturing Company.

B. Sheet Metal Outlet and Device Boxes: Provide minimum 4-inch square by 1-1/2-inch deep, one piece, deep-drawn, galvanized steel, outlet boxes for general use. Provide 4-inch octagonal concrete boxes and hung ceiling boxes of the folded or welded type where required by project conditions. Provide square cornered, straight sided gang boxes wherever required by NFPA 70 or more than two wiring devices are indicated in the same location. Provide boxes of increased depth where required by the project.

1. Construct with stamped knockouts in the back and sides.
2. Provide threaded screw holes with corrosion-resistant screws for securing box covers and wiring devices.
3. All boxes used for systems other than power or lighting shall be 2-1/8” deep minimum.

C. Hinged-Cover Enclosures: NEMA 250, Type 1, with continuous-hinge cover with flush latch, unless otherwise indicated.
   1. Metal Enclosures: Steel, finished inside and out with manufacturer’s standard enamel.

D. Cabinets:
   1. NEMA 250, Type 1, galvanized-steel box with removable interior panel and removable front, finished inside and out with manufacturer’s standard enamel.
   2. Hinged door in front cover with flush latch and concealed hinge.
   3. Key latch to match panelboards.
   4. Metal barriers to separate wiring of different systems and voltage.
   5. Accessory feet where required for freestanding equipment.

2.4 SOURCE QUALITY CONTROL FOR UNDERGROUND ENCLOSURES

A. Handhole and Pull-Box Prototype Test: Test prototypes of handholes and boxes for compliance with SCTE 77. Strength tests shall be for specified tier ratings of products supplied.
   1. Tests of materials shall be performed by an independent testing agency.
   2. Strength tests of complete boxes and covers shall be by either an independent testing agency or manufacturer. A qualified registered professional engineer shall certify tests by manufacturer.
   3. Testing machine pressure gages shall have current calibration certification complying with ISO 9000 and ISO 10012, and traceable to NIST standards.

PART 3 - EXECUTION

3.1 RACEWAY APPLICATION

A. Comply with the following indoor applications, unless otherwise indicated:
   1. Exposed, in equipment rooms, Not Subject to Physical Damage: EMT.
   2. Exposed, Not Subject to Severe Physical Damage: EMT.
   3. Exposed and Subject to Severe Physical Damage: Rigid steel conduit includes raceways in the following locations:
      a. Loading dock.
      b. Corridors used for traffic of mechanized carts, forklifts, and pallet-handling units.
   4. Concealed in Ceilings and Interior Walls and Partitions: EMT.
   5. Connection to Vibrating Equipment (Including Transformers and Hydraulic, Pneumatic, Electric Solenoid, or Motor-Driven Equipment): FMC, except use LFMC in damp or wet locations.
   6. Damp or Wet Locations: IMC.
   7. Raceways for Optical Fiber or Communications Cable in Spaces Used for Environmental Air: EMT.
   8. Exposed in all finished spaces, public places and offices, surface metal raceway, aluminum with aluminum finish.

B. Minimum Raceway Size: ¾-inch (21-mm) trade size.

C. Raceway Fittings: Compatible with raceways and suitable for use and location.
1. Rigid and Intermediate Steel Conduit: Use threaded rigid steel conduit fittings, unless otherwise indicated.
2. PVC Externally Coated, Rigid Steel Conduits: Use only fittings listed for use with that material. Patch and seal all joints, nicks, and scrapes in PVC coating after installing conduits and fittings. Use sealant recommended by fitting manufacturer.

D. Install nonferrous conduit or tubing for circuits operating above 60 Hz. Where aluminum raceways are installed for such circuits and pass through concrete, install in nonmetallic sleeve.

3.2 INSTALLATION OF ELECTRICAL RACEWAYS AND FITTINGS

A. General Installation Requirements:

1. Conduit runs shall be mechanically and electrically continuous from service entrance to all outlets. Each conduit shall enter and be securely connected to a cabinet, junction box, pull box or outlet by means of a locknut on the outside and a bushing on the inside or by means of listed connectors.
2. Conceal conduit, unless indicated otherwise, within finished walls and ceilings, and below floors or finished grade.
3. Keep conduit at least 6 inches away from parallel runs of steam and hot-water pipes.
4. Level and square raceway runs.
5. Install horizontal raceway runs above water and steam piping.
6. Complete installation of electrical raceways before starting installation of cables/wires within raceways.
7. Provide supports for raceways as specified elsewhere in Division 26.
8. Prevent foreign matter from entering raceways; use temporary closure protection, such as push-in or threaded plugs or conduit pennies and bushings. Duct tape is not acceptable.
9. Protect stub-ups from damage where conduits rise from floor slabs. Arrange so curved portion of bends is not visible above the finished slab, nor below the slab where the slab is a finished ceiling.
10. Make bends and offsets so the inside diameter is not effectively reduced.
11. Unless otherwise indicated keep the legs of a bend in the same plane and the straight legs of offsets parallel.
12. Use raceway fittings that are of types compatible with the associated raceway and suitable for the use and location.
13. Run concealed raceways with a minimum of bends. All bends shall have the longest possible radii.
14. Install exposed raceways parallel and perpendicular to nearby surfaces or exposed structural members, and follow the surface contours.
15. Run exposed, parallel or banked raceways together.
16. Make bends in parallel or banked runs from the same center line so that the bends are parallel. Factory elbows may be used in banked runs where they can be installed parallel.
17. Join and terminate raceways with fittings designed and approved for the purpose of the raceway system and make up tight.
18. Where raceways are terminated with locknuts and bushings, align the raceway to enter squarely and install the locknuts so that the dished part is against the box. Use two locknuts, one inside and the other outside the box.
19. Where terminating in threaded hubs, screw the raceway or fitting tight into the hub so the end bears against the wire protection shoulder.
20. Where chase nipples are used, align the raceway and coupling square to the box and tighten the chase nipple so no threads are exposed. Running threads are not allowed.
21. Install pull cords in empty raceways. Provide nylon tape/cord having not less than 200 pounds tensile strength. Leave not less than 12 inches of slack at each end of the pull cord. Label each end of cord with system and destination.

22. Install telephone, data and special systems raceways in accordance with the above requirements for raceway and with the additional requirement that no length of run shall exceed 150 feet for trade sizes one inch and smaller and shall not contain more than three 90-degree bends or the equivalent. Provide pull or junction boxes where necessary to comply with these requirements. Make inside radii of bends in telephone, data and special systems conduits one-inch trade size and larger at least ten times the nominal conduit diameter. Terminate conduit in outlet box and/or with an insulating bushing at all locations.

23. Exposed runs of surface raceway or conduit may be installed only where explicitly permitted. Exposed horizontal runs, where permitted, shall be installed close to ceiling or ceiling beams.

24. Conduits connected to wall outlets shall be run in such a manner that they will not cross water, steam or waste pipes or radiator branches.

25. Conduits and EMT shall not be run through beams, except where clearly indicated on drawings or where permitted.

26. Branch circuit conduits and raceways above suspended ceilings may be supported from the floor construction above or from the main structure support members, however, the finished installation shall not interfere with the removability of ceiling panels. Provide separate support wires independent of ceiling support wires.

B. Flexible Conduit, Steel: Provide flexible conduits for connections to motors and other electrical equipment when it is subject to movement, vibration, misalignment, cramped quarters or where noise transmission is to be eliminated or reduced. Flexible conduit shall be of the liquid-tight type when installed under any of the following conditions:

1. Exterior locations.
2. Moisture or humidity laden atmospheres where it is possible for condensation to accumulate. Corrosive atmospheres.
3. Where water or spray due to wash-operations is frequent or possible. Wherever there is a possibility of seepage or dripping of oil, grease or water.
4. In theatrical areas such as stages, control rooms, catwalks, seating areas, and dimmer rooms.

C. Raceway Sealing Fittings:

1. Sealing fittings for use with threaded steel conduits shall be of the threaded, zinc or cadmium coated, cast or malleable iron type. Fittings used to prevent passage of water vapor shall be of the continuous drain type.
2. In concealed work, install each fitting in a flush steel box with a blank cover plate having a finish similar to that of adjacent plates or surfaces.
3. Provide raceway sealing fittings at the following points, and elsewhere as indicated. Where conduits enter or leave hazardous areas equipped with explosion-proof lighting fixtures, switches, or receptacles. Where conduits pass from warm locations to cold locations, such as refrigerated spaces and air-conditioned spaces. Additionally, provide a brass or stainless steel conduit drain between seal and exterior wall where seal is below grade, where required by the NFPA 70.

D. Surface Metal Raceway:

1. Surface metal raceways shall be used where building construction does not permit concealed wiring methods.
2. Surface metal raceways shall be securely grounded to outlet boxes or to back-plates and fixtures by means of bolts, screws or other approved means.
3. Ends of raceways shall be provided with bushings at entrances to boxes or canopies.
4. A separate green ground conductor shall be installed in the raceway from the junction box supplying the raceway to receptacle or fixture ground terminals.
5. Each surface metal raceway outlet box to which a lighting fixture is attached shall be of sufficient diameter to provide a seat for the fixture canopy.

3.3 INSTALLATION OF CABINETS AND ENCLOSURES

A. Flush Cabinets: Set flush cabinets in finished spaces flush with adjacent walls. Mount cabinets with fronts straight and plumb.

B. Telephone:
1. Install telephone and communications cabinets indicated in corridor walls with bottom just above baseboard.
2. In wire closets, and elsewhere, except as otherwise indicated, install cabinets with tops 6 feet 0 inches above the floor.
3. Install cabinets in finished spaces flush with walls.
4. Install cabinets in unfinished spaces, or where indicated, surface mounted.
5. Install cabinets with fronts straight and plumb.
6. Dimensions for telephone and signal cabinets are minimum sizes of door openings and not the actual box dimensions.

C. Mounting: Mount cabinets at a uniform height, nominally 6 feet 6 inches to the top of the enclosure above finished floor, except as otherwise noted.

D. Support: Support and fasten all cabinets securely in place.

3.4 FIRESTOPPING

A. Apply firestopping to electrical penetrations of fire-rated floor and wall assemblies to restore original fire-resistance rating of assembly.

3.5 PROTECTION

A. Provide final protection and maintain conditions that ensure coatings, finishes, and cabinets are without damage or deterioration at time of Substantial Completion.

1. Repair damage to galvanized finishes with zinc-rich paint recommended by manufacturer.
2. Repair damage to PVC or paint finishes with matching touchup coating recommended by manufacturer.
3. Touch up all welds, scrapes and other mars in the enclosure finish with a rust inhibiting paint and refinish to match enclosure.

END OF SECTION 260533
PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. This Section includes the following:

1. Identification for raceway and metal-clad cable.
2. Identification for conductors and communication and control cable.
4. Warning labels and signs.
5. Instruction signs.
7. Miscellaneous identification products.

B. Codes and Standards: All work accomplished under this section shall comply with the following:

1. Federal Regulations
   b. 29 CFR 1910.145 Specifications for Accident Prevention Signs and Tags

2. American National Standards Institute (ANSI): Comply with requirements of:
   a. ANSI A13.1 Scheme for the Identification of Piping Systems with regard to type and size of lettering for raceway and cable labels.
   b. ANSI C2 National Electric Safety Code (NESC)
   c. ANSI Z535.4 American National Standard for Product Safety Signs and Labels


4. Underwriters Laboratories, Inc. (UL): Comply with requirements of:
   a. 969 Standard For Safety Marking and Labeling Systems

C. Related Sections include the following:

1. Division 26 Section “LOW-VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES" for conductor identification requirements.
2. Division 26 Section “RACEWAY AND BOXES FOR ELECTRICAL SYSTEMS” for identification requirements for raceways, junction boxes and enclosures.
3. Division 26 Section “LOW-VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES for color coding requirements for conductor insulation.
4. Division 26 Section “LOW-VOLTAGE TRANSFORMERS” for equipment labeling requirements.
5. Division 26 Section “SWITCHBOARDS” for equipment labeling requirements.
6. Division 26 Section “PANELBOARDS for equipment labeling requirements.
1.3 SUBMITTALS
   A. Product Data: Submit manufacturer’s data on electrical identification materials and products.
   B. Identification Schedule: An index of nomenclature of electrical equipment and system components used in identification signs and labels.

1.4 COORDINATION
   B. Coordinate installation of identifying devices with completion of covering and painting of surfaces where devices are to be applied.
   C. Coordinate installation of identifying devices with location of access panels and doors.
   D. Install identifying devices before installing acoustical ceilings and similar concealment.

PART 2 - PRODUCTS

2.1 RACEWAY IDENTIFICATION MATERIALS
   A. Comply with ANSI A13.1 for minimum size of letters for legend and for minimum length of color field for each raceway and cable size.
      1. Color for Printed Legends:
         a. Power Circuits: Black letters on an orange field.
         b. Legend: Indicate system or service and voltage, if applicable.
   B. Self-Adhesive Vinyl Labels: Preprinted, flexible label laminated with a clear, weather- and chemical-resistant coating and matching wraparound adhesive tape for securing ends of legend label.
   C. Self-Adhesive Vinyl Tape: Colored, heavy duty, waterproof, fade resistant; 2 inches (50 mm) wide; compounded for outdoor use.

2.2 CONDUCTOR AND COMMUNICATION- AND CONTROL-CABLE IDENTIFICATION MATERIALS
   A. Color-Coding Conductor Tape: Colored, self-adhesive vinyl tape not less than 3 mils (0.08 mm) thick by 1 to 2 inches (25 to 50 mm) wide.
   B. Marker Tapes: Vinyl or vinyl-cloth, self-adhesive wraparound type, with circuit identification legend machine printed by thermal transfer or equivalent process.
   C. Aluminum Wraparound Marker Labels: Cut from 0.014-inch- (0.35-mm-) thick aluminum sheet, with stamped, embossed, or scribed legend, and fitted with tabs and matching slots for permanently securing around wire or cable jacket or around groups of conductors.
   D. Metal Tags: Brass or aluminum, 2 by 2 by 0.05 inch (50 by 50 by 1.3 mm), with stamped legend, punched for use with self-locking nylon tie fastener.
E. Write-On Tags: Polyester tag, 0.010 inch (0.25 mm) thick, with corrosion-resistant grommet and polyester or nylon tie for attachment to conductor or cable.

1. Marker for Tags: Permanent, waterproof, black ink marker recommended by tag manufacturer.

2.3 UNDERGROUND-LINE WARNING TAPE

A. Description: Permanent, bright-colored, continuous-printed, polyethylene tape.

1. Not less than 6 inches (150 mm) wide by 4 mils (0.102 mm) thick.
2. Compounded for permanent direct-burial service.
3. Embedded continuous metallic strip or core (i.e. tracer wire).
4. Printed legend shall indicate type of underground line.

2.4 WARNING LABELS AND SIGNS


B. Self-Adhesive Warning Labels: Factory printed, multicolor, pressure-sensitive adhesive labels, configured for display on front cover, door, or other access to equipment, unless otherwise indicated.

C. Baked-Enamel Warning Signs: Preprinted aluminum signs, punched or drilled for fasteners, with colors, legend, and size required for application. 1/4-inch (6.4-mm) grommets in corners for mounting. Nominal size, 7 by 10 inches (180 by 250 mm).

D. Metal-Backed, Butyrate Warning Signs: Weather-resistant, nonfading, preprinted, cellulose-acetate butyrate signs with 0.0396-inch (1-mm) galvanized-steel backing; and with colors, legend, and size required for application. 1/4-inch (6.4-mm) grommets in corners for mounting. Nominal size, 10 by 14 inches (250 by 360 mm).

E. Warning label and sign shall include, but are not limited to, the following legends:

1. Multiple Power Source Warning: "DANGER - ELECTRICAL SHOCK HAZARD - EQUIPMENT HAS MULTIPLE POWER SOURCES."
2. Workspace Clearance Warning: "WARNING - OSHA REGULATION - AREA IN FRONT OF ELECTRICAL EQUIPMENT MUST BE KEPT CLEAR FOR 36 INCHES (915 MM)."

2.5 INSTRUCTION SIGNS

A. Engraved, laminated acrylic or melamine plastic, minimum 1/16 inch (1.6 mm) thick for signs up to 20 sq. in. (129 sq. cm) and 1/8 inch (3.2 mm) thick for larger sizes.

1. Engraved legend with black letters on white face.
2. Punched or drilled for mechanical fasteners.
3. Framed with mitered acrylic molding and arranged for attachment at applicable equipment.

2.6 EQUIPMENT IDENTIFICATION LABELS

A. Adhesive Film Label: Machine printed, in black, by thermal transfer or equivalent process. Minimum letter height shall be 3/8 inch (10 mm).
B. Adhesive Film Label with Clear Protective Overlay: Machine printed, in black, by thermal transfer or equivalent process. Minimum letter height shall be 3/8 inch (10 mm). Overlay shall provide a weatherproof and ultraviolet-resistant seal for label.

C. Self-Adhesive, Engraved, Laminated Acrylic or Melamine Label: Adhesive backed, with white letters on a dark-gray background. Minimum letter height shall be 3/8 inch (10 mm).

D. Engraved, Laminated Acrylic or Melamine Label: Punched or drilled for screw mounting. White letters on a dark-gray background. Minimum letter height shall be 3/8 inch (10 mm).

E. Stenciled Legend: In nonfading, waterproof, black ink or paint. Minimum letter height shall be 1 inch (25 mm).

2.7 MISCELLANEOUS IDENTIFICATION PRODUCTS

A. Cable Ties: Fungus-inert, self-extinguishing, 1-piece, self-locking, Type 6/6 nylon cable ties.
   1. Minimum Width: 3/16 inch (5 mm).
   2. Tensile Strength: 50 lb (22.6 kg), minimum.
   3. Temperature Range: Minus 40 to plus 185 deg F (Minus 40 to plus 85 deg C).

B. Paint: Paint materials and application requirements are specified in Division 09 painting Sections.
   1. Exterior Concrete, Stucco, and Masonry (Other Than Concrete Unit Masonry):
      a. Semigloss Acrylic-Enamel Finish: Two finish coat(s) over a primer.
         1) Primer: Exterior concrete and masonry primer.
         2) Finish Coats: Exterior semigloss acrylic enamel.

   2. Exterior Concrete Unit Masonry:
      a. Semigloss Acrylic-Enamel Finish: Two finish coat(s) over a block filler.
         1) Block Filler: Concrete unit masonry block filler.
         2) Finish Coats: Exterior semigloss acrylic enamel.

   3. Exterior Ferrous Metal:
      a. Semigloss Alkyd-Enamel Finish: Two finish coat(s) over a primer.
         1) Primer: Exterior ferrous-metal primer.
         2) Finish Coats: Exterior semigloss alkyd enamel.

   4. Exterior Zinc-Coated Metal (except Raceways):
      a. Semigloss Alkyd-Enamel Finish: Two finish coat(s) over a primer.
         1) Primer: Exterior zinc-coated metal primer.
         2) Finish Coats: Exterior semigloss alkyd enamel.

   5. Interior Concrete and Masonry (Other Than Concrete Unit Masonry):
      a. Semigloss Alkyd-Enamel Finish: Two finish coat(s) over a primer.
         1) Primer: Interior concrete and masonry primer.
         2) Finish Coats: Interior semigloss alkyd enamel.

   6. Interior Concrete Unit Masonry:
      a. Semigloss Acrylic-Enamel Finish: Two finish coat(s) over a block filler.
         1) Block Filler: Concrete unit masonry block filler.
         2) Finish Coats: Interior semigloss acrylic enamel.
7. Interior Gypsum Board:
   a. Semigloss Acrylic-Enamel Finish: Two finish coat(s) over a primer.
      1) Primer: Interior gypsum board primer.
      2) Finish Coats: Interior semigloss acrylic enamel.

8. Interior Ferrous Metal:
   a. Semigloss Acrylic-Enamel Finish: Two finish coat(s) over a primer.
      1) Primer: Interior ferrous-metal primer.
      2) Finish Coats: Interior semigloss acrylic enamel.

9. Interior Zinc-Coated Metal (except Raceways):
   a. Semigloss Acrylic-Enamel Finish: Two finish coat(s) over a primer.
      1) Primer: Interior zinc-coated metal primer.
      2) Finish Coats: Interior semigloss acrylic enamel.

C. Fasteners for Labels and Signs: Self-tapping, stainless-steel screws or stainless-steel machine screws with nuts and flat and lock washers.

PART 3 - EXECUTION

3.1 INSTALLATION

A. General Requirements.

1. Coordinate names, abbreviations and other designations used in electrical identification work, with corresponding designations, specified or indicated on drawings. Provide numbers, lettering and wording as approved in submittals, as required by code, or as recommended by manufacturers.
   a. Verify identity of each item before installing identification products.

1. Install products covered by this Section where indicated on drawings or specified. Install products covered by this Section where required by NFPA 70, whether or not otherwise indicated. Install products in accordance with manufacturer's written instructions and requirements of NFPA 70.
2. Location: Install identification materials and devices at locations for most convenient viewing without interference with operation and maintenance of equipment.
   a. Where identification is to be applied to surfaces which require finish, install identification after completion of finish work.
   b. For Self-Adhesive Identification Products: Clean surfaces before application, using materials and methods recommended by manufacturer of identification device.
   c. Attach non-adhesive signs and plastic labels with screws and auxiliary hardware appropriate to the location and substrate.

4. For Painted Identification: Prepare surface and apply paint according to Division 09 painting Sections.

B. Raceway Identification

1. Accessible Raceways and Metal-Clad Cables, 600 V or Less, for Service, Feeder, and Branch Circuits More Than 30 A: Identify with orange self-adhesive vinyl label.
   Accessible Raceways and Cables of Auxiliary Systems: Provide integrally color-coded raceway for all exposed electrical raceway systems installed in accessible areas to assist in system raceway identification. Refer to Division 26 Section "RACEWAY AND BOXES FOR ELECTRICAL SYSTEMS" for additional requirements.

2. All Junction or pullboxes and associated covers installed in non-public spaces associated with special systems shall be painted with similar color coding prior to installation.

3. Raceway colors shall be assigned according to the following color code:

   Fire Alarm System   Red
4. Identification of Junction, Pull and Connection Boxes.
   a. Provide pressure sensitive, self-adhesive labels indicating system voltage in black pre-printed on orange background as required by NFPA 70 for caution signs on all electrical power and lighting system boxes exceeding 4" in length or width in non-public exposed spaces and in concealed locations. Install on outside of box cover.
   b. Label box covers to identify the circuits contained therein. Standard 4 inch square junction box cover plates shall be identified with indelible marker on inside at exposed public locations and on exterior at all other locations.

C. Conductor Identification.

1. Provide color coded insulation for secondary service, feeder and branch circuit conductors throughout the project secondary electrical system as described in Division 26 Section "LOW-VOLTAGE ELECTRICAL POWER CONDUCTORS AND CABLES" for conductor identification requirements.

2. Provide identifying vinyl cloth or aluminum wrap-around marker bands securely fastened to all cables, feeders, and power circuits, pull boxes, junction boxes, panels, switchgear, etc. Provide bands with 1/4-inch letter and number stamps with legend to correspond with designations on drawings. If metal tags are provided, attach them with approximately 55-pound test monofilament line or one piece self-locking nylon cable ties.

3. Tagging or Labeling Conductors: Tag or label conductors as follows:
   a. Tag or label all conductors indicated for future connection (or connection under another contract) with identification indicating source and circuit numbers.
   b. Power-Circuit Conductor Identification: For conductors No. 1/0 AWG and larger in vaults, pull and junction boxes, manholes, and handholes use color-coding conductor tape or metal tags. Identify source and circuit number of each set of conductors. For single conductor cables, identify phase in addition to the above.
   c. Where multiple branch circuits or control wiring or communications/signal conductors are present in the same box or enclosure, (except for 3 circuit, 4 wire home runs), label each conductor or cable. Provide legend indicating source, voltage, circuit number and phase for branch circuit wiring. Phase and voltage of branch circuit wiring may be indicated by means of coded color of conductor insulation. For control and communications/signal wiring use color coding or wire/cable marking tape at terminations and at all intermediate locations where conductors appear in wiring boxes, troughs and control cabinets. Use consistent letter/number conductor designations throughout on wire/cable marking tapes.
   d. Match identification markings with designations used in panelboards, shop drawings, contract documents and similar previously established identification schemes for the facility electrical work.

1. Identify conductors, cables, and terminals in enclosures and at junctions, terminals, and pull points. Identify by system and circuit designation.

2. Use system of marker tape designations that is uniform and consistent with system used by manufacturer for factory-installed connections.


E. Locations of Underground Lines: Identify with underground-line warning tape for power, lighting, communication, and control wiring and optical fiber cable.

   1. Install continuous underground-type plastic line marker with metal tracer, located directly above line at 6 to 8 inches (150 to 200 mm) below finished grade, during backfilling of the trench for each exterior underground power, signal or communication lines.

   2. Where multiple lines are installed in a common trench or concrete envelope and do not exceed an overall width of 16 inches, install a single line marker. Use multiple tapes where width of multiple lines installed in a common trench or concrete envelope exceeds 16 inches (400 mm) overall.

   3. Install line marker for all underground wiring regardless of whether the underground-line is direct-buried or installed in conduit.

F. Warning Labels for Indoor Cabinets, Boxes, and Enclosures for Power and Lighting: Comply with 29 CFR 1910.145 and apply baked-enamel warning signs. Identify system voltage with black letters on an orange background. Apply to exterior of door, cover, or other access.

   1. Equipment with Multiple Power or Control Sources: Apply to door or cover of equipment including, but not limited to, the following:
      a. Power transfer switches.
      b. Controls with external control power connections.

   2. Equipment Requiring Workspace Clearance According to NFPA 70: Unless otherwise indicated, apply to door or cover of equipment but not on flush panelboards and similar equipment in finished spaces.

   3. Where required by NFPA 70, where indicated on drawings or specified, or wherever reasonably required to ensure safe operation and maintenance of electrical systems and of the items to which they connect, install bilingual warning, caution or instruction signs. Where instructions or explanations are needed for system or equipment operation, provide engraved plastic laminate instruction signs with approved legend. For outdoor items provide butyrate signs with metal backing.

   4. For emergency instructions on power transfer, load shedding or other emergency operations, provide engraved laminate signs with approved white legend on red background with minimum 3/8-inch high lettering.

G. Instruction Signs:

   1. Operating Instructions: Install instruction signs to facilitate proper operation and maintenance of electrical systems and items to which they connect. Install instruction signs with approved legend where instructions are needed for system or equipment operation.

H. Equipment Identification Labels: On each unit of equipment, install unique designation label that is consistent with wiring diagrams, schedules, and Operation and Maintenance Manual. Apply labels to disconnect switches and protection equipment, central or master units, control
panels, control stations, terminal cabinets, and racks of each system. Systems include power, lighting, control, communication, signal, monitoring, and alarm systems unless equipment is provided with its own identification.

1. Labeling Instructions:
   a. Indoor Equipment: Engraved, laminated acrylic or melamine label, white lettering in black field. Unless otherwise indicated, provide a single line of text with 1/2-inch- (13-mm-) high letters on 1-1/2-inch- (38-mm-) high label; where 2 lines of text are required, use labels 2 inches (50 mm) high.
   b. Outdoor Equipment: Engraved, laminated acrylic or melamine label.
   c. Elevated Components: Increase sizes of labels and letters to those appropriate for viewing from the floor.

2. Equipment to Be Labeled:
   a. Panelboards, electrical cabinets, and enclosures.
   b. Access doors and panels for concealed electrical items.
   c. Electrical switchgear and switchboards.
   d. Transformers.
   e. Motor-control centers.
   f. Disconnect switches.
   g. Enclosed circuit breakers.
   h. Motor starters.
   i. Push-button stations.
   j. Power transfer equipment.
   k. Contactors.
   l. Remote-controlled switches, dimmer modules, and control devices.
   m. Battery inverter units.
   n. Power-generating units.
   o. Voice and data cable terminal equipment.
   p. Fire-alarm control panel and annunciators.
   q. Security and intrusion-detection control stations, control panels, terminal cabinets, and racks.
   r. Intercom system master station equipment
   s. Monitoring and control equipment.
   t. Uninterruptible power supply equipment.
   u. Terminals, racks, and patch panels for voice and data communication and for signal and control functions.

3. Provide circuit source/control source/item description designation labels of engraved plastic laminate for all disconnect switches, breakers, pushbuttons, pilot lights, motor controls and similar items for all power distribution and control components above, except panelboards and alarm/signal components, where labeling is specified elsewhere.

4. Install labels at locations as indicated on drawings or as specified. Where not so designated, install labels at locations for best convenience of viewing without interference with operation and maintenance of equipment.

5. Provide 480/277-volt panelboards with “480/277 VOLTS” in 2-inch high yellow letters on inside of cabinet doors.

6. For panelboards, furnish and install a neat metal directory frame with 1/16 inch plastic cover on the inside of each panel cabinet door.
a. Provide typewritten list of the complete circuits in the directory frames, showing portions of building or equipment supplied by each circuit.
   1) Minimum card size, 5" x 8" for panels up to 20 circuits; 2 cards above 20 circuits.
   2) Numbering odd down left hand side, and even down right. See drawings for panel schedules.
   3) The directory shall contain the following detailed information: type(s) of circuit served, room number(s) served, with "actual" room numbers to be used after completion of project.

END OF SECTION
SECTION 280500
COMMON WORK RESULTS FOR ELECTRONIC SAFETY AND SECURITY

PART 1 - GENERAL

1.1 RELATED DOCUMENTS
A. Drawings and general provisions of the Contract, including General and Supplementary Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY
A. Section Includes:
   1. Electronic safety and security equipment coordination and installation.
   2. Common electronic safety and security installation requirements.

1.3 COORDINATION
A. Coordinate arrangement, mounting, and support of electronic safety and security equipment:
   1. To allow maximum possible headroom unless specific mounting heights that reduce headroom are indicated.
   2. To provide for ease of maintaining the equipment with minimum interference to other installations.
   3. To allow right of way for piping and conduit installed at required slope.
   4. So connecting raceways, cables, wireways, cable trays, and busways will be clear of obstructions and of the working and access space of other equipment.
B. Coordinate installation of required supporting devices and other structural components as they are constructed.
C. Coordinate location of access panels and doors for electronic safety and security items that are behind finished surfaces or otherwise concealed.

PART 2 - PRODUCTS ( NOT USED )

PART 3 - EXECUTION

3.1 COMMON REQUIREMENTS FOR ELECTRONIC SAFETY AND SECURITY 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 maintenance with minimum interference with other items in the vicinity.

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

F. Interior Penetrations of Non-Fire-Rated Walls and Floors: Seal annular space between sleeve and raceway or cable, using joint sealant appropriate for size, depth, and location of joint.

G. Fire-Rated-Assembly Penetrations: Maintain indicated fire rating of walls, partitions, ceilings, and floors at raceway and cable penetrations. Install sleeves and seal raceway and cable penetration sleeves with firestop materials.

3.2 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.

END OF SECTION 280500
SECTION 280513

CONDUCTORS AND CABLES FOR ELECTRONIC SAFETY AND SECURITY

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including General and Supplementary
   Conditions and Division 01 Specification Sections, apply to this Section.

1.2 SUMMARY

A. Section Includes:
   1. RS-232 cabling.
   2. RS-485 cabling.
   3. Low-voltage control cabling.
   5. Identification products.

1.3 DEFINITIONS


B. EMI: Electromagnetic interference.

C. IDC: Insulation displacement connector.

D. 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.

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

F. RCDD: Registered Communications Distribution Designer.

1.4 SUBMITTALS

A. Product Data: For each type of product indicated.

   1. For cable, include the following installation data for each type used:

      a. Nominal OD.
      b. Minimum bending radius.
      c. Maximum pulling tension.

B. Qualification Data: For qualified layout technician, installation supervisor, and field inspector.
C. Field quality-control reports.

D. Operation and Maintenance Data: For wire and cable to include in operation and maintenance manuals. In addition to items specified in Division 01 Section "Operation and Maintenance Data," include the following:

1. Allowable pulling tension of cable.
2. Cable connectors and terminations recommended by the manufacturer.

1.5 QUALITY ASSURANCE

A. Testing Agency Qualifications: An NRTL.

1. Testing Agency's Field Supervisor: Currently certified by BICSI as an RCDD to supervise on-site testing.

B. Surface-Burning Characteristics: As determined by testing identical products according to ASTM E 84 by a qualified testing agency. Identify products with appropriate markings of applicable testing agency.

1. Flame-Spread Index: 25 or less.
2. Smoke-Developed Index: 450 or less.

C. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

1.6 DELIVERY, STORAGE, AND HANDLING

A. Test cables upon receipt at Project site.

1.7 PROJECT CONDITIONS

A. Do not install conductors and cables that are wet, moisture damaged, or mold damaged.

1. Indications that wire and cables are wet or moisture damaged include, but are not limited to, discoloration and sagging of factory packing materials.

B. Environmental Limitations: Do not deliver or install 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.

PART 2 - PRODUCTS

2.1 PATHWAYS

A. Support of Open Cabling: NRTL labeled for support of cabling, designed to prevent degradation of cable performance and pinch points that could damage cable.
1. Support brackets with cable tie slots for fastening cable ties to brackets.
2. Lacing bars, spools, J-hooks, and D-rings.
3. Straps and other devices.

B. Conduit and Boxes: Comply with requirements in Division 26 Section "Raceway and Boxes for Electrical Systems."

C. Outlet boxes shall be no smaller than 2 inches wide, 3 inches, and 2-1/2 inches deep.

2.2 CABLE, HYBRID POWER AND CONTROL

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:

1. ADC.
2. AMP Netconnect; a brand of Tyco Electronics Corporation.
3. Belden CDT Networking Division/NORDX.
4. Belden Inc.
5. Berk-Tek; a Nexans company.
6. CommScope, Inc.
7. Draka Cableteq USA.
8. Genesis Cable Products; Honeywell International, Inc.
9. Mohawk; a division of Belden.
10. Superior Essex Inc.
11. SYSTIMAX Solutions; a CommScope, Inc. brand.
12. 3M; Communication Markets Division.

2.3 RS-232 CABLE

A. Plenum-Rated Cable: NFPA 70, Type CMP, integrated into hybrid cable.

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.
5. Pairs are cabled on common axis with No. 24 AWG, stranded (7x32) tinned copper drain wire.

2.4 RS-485 CABLE

A. Plenum-Rated Cable: NFPA 70, Type CMP, integrated into hybrid cable

1. Paired, No. 22 AWG, stranded (7x30) tinned copper conductors.
2. Fluorinated ethylene propylene insulation.
3. Unshielded.
4. Fluorinated ethylene propylene jacket.
2.5  LOW-VOLTAGE CONTROL CABLE

A. Plenum-Rated, Paired Cable: NFPA 70, Type CMP, integrated into hybrid cable.

1. Twisted, tinned copper conductors.
2. Flame Resistance: Comply with NFPA 262.

2.6  CONTROL-CIRCUIT CONDUCTORS

A. General Wire and Cable Requirements: NRTL listed and labeled as complying with NFPA 70, Article 760.

2.7  IDENTIFICATION PRODUCTS

A. Manufacturers: Subject to compliance with requirements, provide products by one of the following:

1. Brady Corporation.
2. HellermannTyton.
3. Kroy LLC.
4. PANDUIT CORP.

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

C. Comply with requirements in Division 26 Section "Identification for Electrical Systems."

2.8  SOURCE QUALITY CONTROL

A. Testing Agency: Engage a qualified testing agency to evaluate cables.

B. Factory test cables on reels according to TIA/EIA-568-B.1.

C. Factory test cables according to TIA/EIA-568-B.2.

D. Factory test multimode optical fiber cables according to TIA-526-14-A and TIA/EIA-568-B.3.

E. Cable will be considered defective if it does not pass tests and inspections.

F. Prepare test and inspection reports.

PART 3 - EXECUTION

3.1  INSTALLATION OF PATHWAYS

A. Cable Trays: Comply with NEMA VE 2 and TIA-569-B.

B. Comply with TIA-569-B for pull-box sizing and length of conduit and number of bends between pull points.
3. Comply with requirements in Division 26 Section "Raceway and Boxes for Electrical Systems." for installation of conduits and wireways.

D. Install manufactured conduit sweeps and long-radius elbows whenever possible.

3.2 INSTALLATION OF HANGERS AND SUPPORTS

A. Comply with requirements in Division 26 Section "Hangers and Supports for Electrical Systems." for installation of supports for pathways, conductors and cables.

3.3 WIRING METHOD

A. 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. Control and data transmission wiring shall not share conduit with other building wiring systems.

B. 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.

3.4 INSTALLATION OF CONDUCTORS AND CABLES

A. Comply with NECA 1.

B. Conductors: Size according to system manufacturer's written instructions unless otherwise indicated.

C. General Requirements for Cabling:

2. Comply with BICSI ITSIM, Ch. 6, "Cable Termination Practices."
3. Terminate all conductors; no cable shall contain unterminated elements. Make terminations only at indicated outlets, terminals, and cross-connect and patch panels.
4. 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.
5. 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.
6. 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.
7. Cold-Weather Installation: Bring cable to room temperature before dereeling. Heat lamps shall not be used for heating.
8. Pulling Cable: Comply with BICSI ITSIM, Ch. 4, "Pulling Cable." Monitor cable pull tensions.
D. Cable Installation: Install using techniques, practices, and methods that are consistent with rating of components and that ensure performance of completed and linked signal paths, end to end.

2. Install 110-style IDC termination hardware unless otherwise indicated.
3. Do not untwist cables more than 1/2 inch from the point of termination to maintain cable geometry.

E. 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 above ceilings by cable supports not more than 60 inches apart.
3. Cable shall not be run through structural members or in contact with pipes, ducts, or other potentially damaging items.

F. Separation from EMI Sources:

1. Comply with BICSI TDMM and TIA-569-B 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:
   b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 12 inches.
3. Separation between communications cables in grounded metallic raceways and unshielded power lines or electrical equipment shall be as follows:
   b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 6 inches.
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:
   b. Electrical Equipment Rating between 2 and 5 kVA: A minimum of 3 inches.
5. Separation between Cables and Electrical Motors and Transformers, 5 kVA or HP and Larger: A minimum of 48 inches.

3.5 FIRESTOPPING

A. Comply with TIA-569-B, "Firestopping" Annex A.
B. Comply with BICSI TDMM, "Firestopping Systems" Article.

3.6 GROUNDING


B. For low-voltage wiring and cabling, comply with requirements in Division 26 Section "Grounding and Bonding for Electrical Systems."

3.7 IDENTIFICATION

A. Identify system components, wiring, and cabling complying with TIA/EIA-606-A. Comply with requirements for identification specified in Division 26 Section "Identification for Electrical Systems."

3.8 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 cable jacket materials for NRTL certification markings. Inspect cabling terminations to confirm color-coding for 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. Test cabling for DC loop resistance, shorts, opens, intermittent faults, and polarity between conductors. Test cables after termination.

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.

END OF SECTION 280513
SECTION 285000
SECURITY MANAGEMENT SYSTEM

PART 1 - GENERAL

1.1 CONDITIONS AND REQUIREMENTS
   A. The General Conditions, Supplementary Conditions, and Division 01 – General Requirements apply.

1.2 SECTION INCLUDES
   A. General description, functional requirements, operational characteristics, and criteria for the Security Management System (SMS) to include door access improvements described in the Contract Documents.

1.3 RELATED SECTIONS
   A. Division 26 - Electrical: Electrical systems and components.
   B. Section 28 05 13 - Conductors and Cables for Electronic Safety and Security.

1.4 DEFINITIONS
   A. API: Application Programming Interface.
   C. NTSC: National Television Standards Committee.
   D. PAL: Phase Alternating Line. PAL is the color video standard used in Europe and many other countries.
   E. SMS: Security Management System.

1.5 REFERENCE STANDARDS
   A. Where more than one (1) reference standard, code, or regulation applies, the more stringent one shall govern.
   B. Electronic Industries Alliance (EIA):
      1. EIA RS-170 - Standard for Composite Video Signals.
   C. Federal Communications Commission (FCC):
      1. FCC Part 15 - Unlicensed RF Devices.
2. FCC Part 68 - Requirements for Connecting to the U.S. Phone Network.

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

E. International Organization for Standardization (ISO).

F. International Radio Consultive Committee (CCIR).

G. Microsoft® Open Database Connectivity (ODBC) Interface.

H. National Fire Protection Association (NFPA):

1. NFPA 70 - National Electrical Code.

I. National Institute of Standards and Technology (NIST):


J. National Television Standards Committee (NTSC):


K. Underwriters Laboratories Inc. (UL):

1. UL 294 - Standard for Access Control System Units.
2. UL 1076 - Standard for Proprietary Burglar Alarm Units and Systems.

L. Underwriters Laboratories of Canada (ULC).

1.6 SECURITY MANAGEMENT SYSTEM (SMS) DESCRIPTION

A. The Security Management System (SMS) outlined in this section and detailed in Part 2 of this section is the key central component for managing physical security and the bridge between physical and logical security for a project. The system shall provide a variety of integral functions including: regulation of access and egress; provision of identification credentials; and monitor, track and interface alarms. Future projects may implement viewing, recording and storage of digital surveillance video linked to SMS events.

B. The SMS shall utilize a single seamlessly integrated relational database for all functions utilizing a fully multi-tasking multi-threading Microsoft Windows 7 or 2008 or Vista or XP or 2003 Operating System. The SMS shall be written so that all system modules (access control, alarm monitoring, ID or credential management, visitor management, asset management and digital video management) are developed and built from a unified single 32-bit source code set. Separate source code bases for individual modules of the SMS are not acceptable.

C. Upgrades or expansion of the SMS to a larger size system in scale shall not require installation of a different and/or new SMS application or require the administrator or operator to learn a different and or new interface from the previous version.

D. The SMS shall be written using Unicode format. Unicode enables a single software product to be targeted across multiple platforms and languages without re-engineering and allows for data to be transported through different systems without corruption. The SMS graphical user
interface shall be available in the following single-byte languages: Arabic (ARA), Croatian (HRV), Czech (CSY), Dutch (NLD), English (ENU), Finnish (FIN), French (FRA), German (DEU), Hebrew (HEB), Italian (ITA), Polish (PLK), Portuguese Brazil (PTB), Russian (RUS), Spanish (ESP), and Swedish (SVE). The SMS graphical user interface shall be available in the following double-byte languages: Chinese Simplified (CHS), Chinese Traditional (CHT), Korean (KOR), and Japanese (JPN). Language Accessory Add-ons shall require a special language-specific license bit in order for the Language Pack to be used.

E. The SMS software developer shall be a Microsoft Gold Certified Partner.

F. The SMS shall be Microsoft Windows XP Certified.

G. The SMS shall be compatible with Microsoft Windows 7, and shall have passed Microsoft-designed tests for compatibility and reliability on Windows 7.

H. The SMS shall be UL 1076 Listed (pending).

I. The SMS shall have FIPS 140-2 certification (pending).

J. The SMS shall only require a single license key to be present on the database server for the SMS to operate. The license key shall either be a physical device or a software license key. The SMS shall allow the SMS USER the ability to activate, return, or repair the software license key. The software license shall only be used on a physical computer or in a VMware virtual environment. License keys shall not be required at the client workstations. The license key on the database server shall determine the number of client workstations that shall be able to connect to the SMS as well as all SMS functionality. An alarm shall be generated in the SMS’s Alarm Monitoring application as the license expiration date approaches.

K. The License Administration login and password shall be encrypted when they are passed to the License Server. The hash shall not be the same data even with the same logon credentials on different systems. This is a requirement for U.S. government DIACAP certification.

L. The SMS shall support concurrent licensing with respect to client licenses. CUSTOMER shall purchase a fixed number of client workstation licenses (or connections) that shall be programmed into the database server license file. The SMS shall be installed on any number of client workstations in the CUSTOMER facility. Then, any of the client workstations that have the SMS software installed shall have the ability to connect to the database server as long as the maximum number of concurrent connections purchased has not been reached. Connections shall be licensed on a per module basis. This shall provide CUSTOMER with great flexibility in system design and layout.

M. The SMS shall provide support for single sign-on capability. Single sign-on shall allow System Administrators/System Operators to authenticate into SMS applications using their Windows domain account.

Single sign-on shall support the following scenarios:

1. Allow System Administrators/System Operators to interactively run SMS applications without having to enter a username or password. This shall make administration of the SMS easier since maintenance of separate SMS usernames and passwords is not required.

2. Allow SMS API scripts to authenticate. These scripts shall be run using a Windows account allowing a seamless and secure way to authenticate the account and restricting the script to those actions that the user is permitted to perform.
N. The SMS shall be able to seamlessly interface with and monitor intelligent system controllers, reader interface modules, I/O panels, alarm panels, alarm panel receivers, biometric devices, personal protection devices, intercom systems, fire alarm panels (secondary monitoring only), building management systems and digital video recorders approved for use by the SMS manufacturer.

O. The SMS shall be able to communicate with intelligent system controllers via RS-485, RS-232, TCP/IP or Ethernet, and dialup via modem.

P. Tasks shall be accessible from any compatible client workstation on the network utilizing one (1) or all of the following:

1. Traditional client-server architecture.
2. N-tier architecture where the SMS supports the expansion of the system architecture and allows for user deployment based upon their system architectural needs. The SMS shall allow for, but not require, the separation of the database, application server, Web server, and client interface. The system shall require that all connections to the database be performed through a trusted link from the client or internet browser interface.
3. Centralized distribution (publishing) of applications using Windows Terminal Server and Citrix® on Windows, UNIX, Linux or Apple Macintosh based systems through any compatible internet browser application and/or by means of a mobile computing platform using a wearable computer, Tablet PC, or PDA device.

Q. Utilize an open architecture where all data must reside on a single database and must be accessible in real time to SMS workstation or Web-based client connected to the network. The system shall be configurable to support all of the following databases: Microsoft SQL Server 2008, Microsoft SQL Server 2005, Oracle Server 11g, and Oracle Server 10g. Oracle data may reside on Windows or UNIX platforms.

R. The system architecture shall support Microsoft Windows Clustering, Hot Standby, Fault Tolerant Servers and Fault Tolerant Hot Standby Servers.

S. The SMS shall be able to connect to and interface bi-directionally with external data sources utilizing all of the following methods:

1. ASCII with support for XML formatted text exchange of data activated both manually and automatically.
2. ASCII with support for XML formatted text exchange of data using a direct table interface activated both manually and automatically.
3. Real-time exchange of data via Active Directory or LDAP utilizing an API (Application Programming Interface) written by the SMS manufacturer. The live exchange of data shall expose SMS events and transactions to other data sources in real-time and allow for receipt of data into the SMS where this data may be acted upon and trigger linked events in the SMS in real-time.

T. The SMS shall support:

1. Lenel OnGuard® PRO Series: Unlimited number of access control readers, unlimited number of inputs or outputs, unlimited number of client workstations, unlimited number of cardholders.

U. All Video surveillance equipment, cabling, DVR Units, cameras, etc. are future, N. I. C., but SMS Architecture shall include required interface for said future equipment.
1.7 SUBMITTALS

A. Submit under provisions of Section 01 33 00.

B. Product Data: For each type of product indicated. Include rated capacities, operating characteristics, and furnished specialties and accessories. Reference each product to a location on Drawings.

1. Manufacturer’s technical data for all material and equipment at the system and sub-system level to be provided as part of the SMS.
2. A system description including analysis and calculations used in sizing equipment required by the SMS. The description shall show how the equipment will operate as a system to meet the performance requirements of the SMS. The following information shall be supplied as a minimum:
   a. Server(s) processor(s), disk space and memory size.
   b. Description of site equipment and its configuration.
   c. Network bandwidth, latency and reliability requirements.
   d. Backup or archive system size and configuration.
   e. Start up operations.
   f. System expansion capability and method of implementation.
   g. System power requirements and UPS sizing.
   h. Device or component environmental requirements (cooling and or heating parameters).
   i. A description of the operating system and application software.

C. Shop Drawings: Submit plans, elevations, sections, details, and attachments to other work.

1. Indicate all system device locations on architectural floor plans. No other system(s) shall be included on these plans.
2. Include full schematic wiring information on these drawings for all devices. Wiring information shall include cable type, conductor routings, quantities, and connection details at device.
3. Include a complete SMS one-line, block diagram.
4. Include a statement of the system sequence of operation.

D. Operation and Maintenance Data: For electronic security system to include in emergency, operation, and maintenance manuals. In addition to items specified in Section 01, include the following:

1. Provide 2 sets electronic format manuals including operating instructions, maintenance recommendations and parts list including wiring and connection diagrams modified to reflect as-built conditions.
2. Manuals: Deliver final copies of the manuals within 14 days after completing the installation test. Each manual’s contents shall be identified on the cover. The manual shall include names, addresses, and telephone numbers of the Contractor responsible for the installation and maintenance of the system and the factory representatives for each item of equipment for each system. The manuals shall have a table of contents and labeled sections. The final copies delivered after completion of the installation test shall include all modifications made during installation, checkout, and acceptance testing. The manuals shall consist of the following:
   a. Functional Design Manual: Identify the operational requirements for the system and explain the theory of operation, design philosophy, and specific functions.
Include a description of hardware and software functions, interfaces, and requirements.

b. Hardware Manual: Describe equipment furnished including:

1) General description and specifications.
2) Installation and check out procedures.
3) Equipment layout and electrical schematics to the component level.
4) System layout drawings and schematics.
5) Alignment and calibration procedures.
6) Manufacturer’s repair parts list indicating sources of supply.

c. Software Manuals: Describe the functions of software and include all other information necessary to enable proper loading, testing, and operation. The manual shall include:

1) Definition of terms and functions.
2) System use and application software.
3) Initialization, startup, and exit.
4) Reports generation.
5) Details on forms customization and field parameters.

3. As-Built Drawings: During system installation, the Contractor shall maintain a separate hard copy set of drawings, elementary diagrams, and wiring diagrams of the SMS to be used for record drawings. This set shall be accurately kept up to date by the Contractor with all changes and additions to the SMS. Copies of the final as-built drawings shall be provided to the end user in DXF format.

1.8 QUALITY ASSURANCE

A. Manufacturer Qualifications:

1. SMS manufacturer shall be an established organization with referenced and documented experience delivering and maintaining SMS of equal or higher sophistication and complexity as compared to the system detailed in this specification.
2. SMS manufacturer shall employ at a minimum the following methods for quality assurance of component and assembly devices.
   a. Perform visual inspection of devices to verify assembly according to defined procedures. Perform end of line operational tests to ensure product functionality has been correctly configured.
   3. Perform individual functionality and system level regression testing to ensure compliance with product specifications. Perform single and multiple unit system tests to mimic end-user installation configurations. Utilize automated hardware and software testing to evaluate system performance under published operational loads and compare to published system capabilities.

B. Bidder Qualifications:

1. At the time of the bid, the bidder shall have satisfactorily completed projects of a similar size, scope and complexity as the system detailed in this specification. The bidder shall furnish written proof of experience from three (3) references and proof of current
accreditation or certification by the manufacturer for required training for sales or installation or service of the SMS and associated devices.

2. The bidder shall also be a factory authorized local service organization that shall carry a complete stock of parts and provide maintenance for the SMS and related systems under this contract. Local shall be defined as an area in a 50 mile radius of installed location.

1.9 DELIVERY, STORAGE AND HANDLING

A. Deliver, store, and handle materials, components, and equipment in manufacturer's protective packaging.

B. Store components and equipment in temperature and humidity controlled environment in original manufacturer's sealed containers. Maintain ambient temperature between 50 and 85 degrees Fahrenheit (10 and 29.4 degrees Celsius), and not more than 80 percent relative humidity, non-condensing.

C. Open each package; verify contents against packing list; and file copy of packing list, complete with package identification, for inclusion in operation and maintenance data.

D. Mark packing list with the same designations assigned to materials, components, and equipment for recording in the system labeling schedules that are generated by software.

E. Save original manufacturer's containers and packing materials and deliver as directed under provisions covering extra materials.

1.10 PROJECT CONDITIONS

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

1. Equipment and Components: Rated for continuous operation in ambient conditions of 60 to 85 degrees Fahrenheit (15.5 and 29.4 degrees Celsius) and a relative humidity of 20 to 80 percent, non-condensing.

2. Indoor, Controlled Environment: NEMA 250, Type 1 enclosure. System components, except the central-station control unit, installed in temperature-controlled indoor environments shall be rated for continuous operation in ambient conditions of 85 dry bulb and 20 to 90 percent relative humidity, non-condensing.

1.11 WARRANTY

A. SMS, Third-party, and Access Control Warranty:

1. SMS manufacturer warrants that the product disc and hardware key shall be free from defects in material and workmanship and that SMS software product will function in substantial accordance to SMS manufacturer's specifications. Any defective dongle will be replaced at no charge provided that the system is currently on a supported version of SMS software. Dongles for non-supported versions will be replaced for a cost.

2. All SMS manufacturer branded access control hardware are provided with a three (3) year warranty from the date of shipment to the Reseller. SMS manufacturer warrants that such products will be free from defects in material and workmanship and that they will operate in general accordance with their product specifications. The parts will be repaired or replaced at the manufacturer's option. Reseller shall follow SMS manufacturer's
procedures for RMA with these products. SMS manufacturer provides repair or replacement of SMS manufacturer branded components for up to five years from the product discontinuance date.

3. Transfer SMS third-party device warranties from the manufacturer to the Contractor, which may then transfer third-party warranties to the Owner. Specific third-party warranty details, terms and conditions, remedies and procedures, are either expressly stated on, or packaged with, or accompany such products. The warranty period may vary from product to product. These products include but are not limited to devices that are directly interconnected to the SMS field hardware or computers and are purchased directly from the SMS manufacturer. Examples may include but not be limited to: credential printers, reader heads, biometric devices, computers, etc.

PRODUCTS

1.12 MANUFACTURERS


B. Substitutions will be considered under provisions of Section 01.

1.13 SMS SOFTWARE

A. Security Management System (SMS) Software: Lenel Systems International “OnGuard” Series PRO.

1.14 SMS FIELD HARDWARE

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

1. Intelligent System Controllers (ISC): LNL-500 or LNL-2220 or LNL-3300
2. Intelligent Single Door Controller: LNL-2210
3. Intelligent Dual Reader Controller
4. Integrated Access and Intrusion System Controller: NGP Controller
5. Input Control Module (ICM): LNL-1100
6. Output Control Module (OCM): LNL-1200
7. Single Reader Interface Module (SRI): LNL-1300
8. Dual Reader Interface Module (DRI): LNL-1320
9. Biometric Reader Interface Gateway: LNL-500B
10. Access Control Network Door Controllers or Network Controller/Readers
11. Wireless Gateway Interface: LNL-500W
12. ISC Display Timer
13. Network Adapters
14. Dialup Modems
15. Communication Star Multiplexer: LNL-8000
16. Power supplies and enclosures
17. UL, CUL, and CE listed power supplies and enclosures

B. SMS Authentication Hardware:
1. Lenel OpenCard or OpenProx Readers
2. Lenel OpenCard-Secure or OpenProx Readers

C. SMS Credential Printers: The SMS credential management module shall be compatible with printers and printer or encoder from Zebra, Magicard, and NiSCA that support Microsoft Certified Windows 2003 and XP drivers. The SMS shall support double-sided full color printing on printers that have that capability. The SMS shall also support edge-to-edge printing on printers that have that capability. The SMS shall support high-speed printing on printers that have that capability. The SMS shall also support holographic overlays on printers that have that capability. Allow for 1,000 credentials under the Base Bid.

D. SMS Third-party Devices: The SMS shall interface with select devices from the following manufacturers:

1. Osborne Hoffman 2020
2. Pyrotronics MXL fire panel
3. Pyrotronics MXL-IQ fire panel
4. Notifier AM2020 fire panel
5. Notifier NFS-640 fire panel
6. Ericsson MD110 PBX
7. AES Intellinet
8. OMNIKEY Smart card readers
9. Otis Compass Destination Entry System version 1.0

1.15 SERVER AND WORKSTATION REQUIREMENTS

A. Database Servers

1. Servers for Windows 2008 or 2003 Access Control and Alarm Monitoring Systems
   a. Dell PowerEdge R710
   b. Intel® Xeon® E5520, 2.26Ghz, 8M Cache, Turbo, HT, 1066MHz
   c. 4GB Memory (2x2GB), 1066MHz Dual Ranked UDIMMs for 1 Processor, Adv ECC
   d. 24X IDE CD-RW/DVD ROM Drive
   e. 160GB 7.2K RPM SATA 2.5" Hot Plug Hard Drive for Operating System
   f. 160GB 7.2K RPM SATA 2.5" Hot Plug Hard Drive for Database
   g. RD1000 Backup, Internal SATA Drive Bay for 2.5" Chassis
   h. RD1000 Internal Removable Hard Disk for RD1000, 160GB Native / 320GB Comp
   i. Four 10/100/1000 Ethernet Network Ports
   j. 17 in. Flat LCD Monitor
   k. Onboard VGA
   l. 1 serial port
   m. 6 USB 2.0 ports
   n. Speakers
   o. USB Keyboard
   p. USB Optical Mouse
   q. Surge Suppression Strip
   r. Microsoft Windows Server 2008 or 2003 Operating System
   s. Microsoft SQL Server 2008 or 2005 Relational Database Management System
   t. SMS Server Software for Windows 2008 or 2003
2. Servers for Windows 2008 or 2003 PRO Access Control and Alarm Monitoring Systems
   a. Dell PowerEdge R710
   b. Intel® Xeon® E5520, 2.26Ghz, 8M Cache, Turbo, HT, 1066MHz Max Mem
   c. 4GB Memory (2x2GB), 1066MHz Dual Ranked UDIMMs for 1 Processor, Adv ECC
   d. 24X IDE CD-RW/DVD ROM Drive
   e. 160GB 7.2K RPM SATA 2.5" Hot Plug Hard Drive for Operating System
   f. 160GB 7.2K RPM SATA 2.5" Hot Plug Hard Drive for Database
   g. RD1000 Backup, Internal SATA Drive Bay for 2.5" Chassis
   h. RD1000 Internal Removable Hard Disk for RD1000, 160GB Native/320GB Comp
   i. Four 10/100/1000 Ethernet Network Ports
   j. Onboard VGA
   k. 17 in. Flat LCD Monitor
   l. 1 serial port
   m. 6 USB 2.0 ports
   n. Speakers
   o. USB Keyboard
   p. USB Optical Mouse
   q. Surge Suppression Strip
   r. Microsoft Windows Server 2008 or 2003
   s. Microsoft SQL Server 2008 or 2005 Relational Database Management System
   t. SMS Server Software for Windows 2008 or 2003

   a. Dell PowerEdge R710
   b. Intel® Xeon® E5520, 2.26Ghz, 8M Cache, Turbo, HT, 1066MHz Max Mem
   c. 4GB Memory (2x2GB), 1066MHz Dual Ranked UDIMMs for 1 Processor, Adv ECC
   d. 24X IDE CD-RW/DVD ROM Drive
   e. 160GB 7.2K RPM SATA 2.5" Hot Plug Hard Drive for Operating System
   f. 160GB 7.2K RPM SATA 2.5" Hot Plug Hard Drive for Database
   g. RD1000 Backup, Internal SATA Drive Bay for 2.5" Chassis
   h. RD1000 Internal Removable Hard Disk for RD1000, 160GB Native/320GB Comp
   i. Four 10/100/1000 Ethernet Network Ports
   j. Onboard VGA
   k. 17 in. Flat LCD Monitor
   l. 1 serial port
   m. 6 USB 2.0 ports
   n. Speakers
   o. USB Keyboard
   p. USB Optical Mouse
   q. Surge Suppression Strip
   r. Microsoft Windows Server 2008 or 2003 Operating System
   s. Microsoft SQL Server 2008 or 2005 Relational Database Management System
   t. SMS Server Software for Windows 2008 or 2003

4. Servers for Windows 2008 or 2003 Integrated Systems
   a. Dell PowerEdge R710
   b. Intel® Xeon® E5520, 2.26Ghz, 8M Cache, Turbo, HT, 1066MHz Max Mem
   c. 4GB Memory (2x2GB), 1066MHz Dual Ranked UDIMMs for 1 Processor, Adv ECC
   d. 24X IDE CD-RW/DVD ROM Drive
   e. 160GB 7.2K RPM SATA 2.5" Hot Plug Hard Drive for Operating System
   f. 160GB 7.2K RPM SATA 2.5" Hot Plug Hard Drive for Database
   g. RD1000 Backup, Internal SATA Drive Bay for 2.5" Chassis
   h. RD1000 Internal Removable Hard Disk for RD1000, 160GB Native/320GB Comp
   i. Four 10/100/1000 Ethernet Network Ports
   j. Onboard VGA
B. Client Workstations PC Specifications

1. Client Workstations for Windows 2008 or 2003 SYSTEMS
   a. Intel Pentium 4 Dual Core E2180, 2.0GHz, 1M L2 Cache, 800FSB
   b. 1GB non-ECC, 667MHz DDR2 1x1GB (1DIMM)
   c. 24X CD-RW/DVD Combo Drive
   d. 80GB SATA II 3.0Gb/s, 8MB Cache, 7200 RPM hard drive
   e. 10/100/1000 Ethernet Network Port
   f. 1 serial port
   g. 1 parallel port
   h. 17 in. Flat LCD Monitor
   i. 64 MB Video Card
   j. Speakers
   k. USB Keyboard
   l. USB Optical Mouse
   m. Surge Suppression Strip
   n. Microsoft Windows XP or Vista
   o. Microsoft SQL Server 2008 or 2005 Client License
   p. SMS Client Software for Windows XP or Vista

2. System Administration only
   a. Dell OptiPlex 780 Small Form Factor
   b. Intel® Pentium® Dual Core E5300 with VT (2.60GHz, 2M, 800MHz FSB)
   c. 4GB DDR3 Non-ECC SDRAM, 1066MHz, (4 DIMM)
   d. 8X Slimline DVD+/-RW
   e. 160GB 7,200 RPM 3.5" SATA, 3.0Gb/s Hard Drive with NCQ and 8MB Cache
   f. 10/100/1000 Ethernet Network Port
   g. 1 serial port
   h. 1 parallel port
   i. 19 in. Flat LCD Monitor
   j. Integrated Video, Intel® GMA 4500
   k. Internal Chassis Speakers
   l. USB Keyboard
   m. USB Optical Mouse
   n. Surge Suppression Strip
   o. Microsoft Windows 7
   p. Microsoft SQL Server 2008 Client License
   q. SMS Client Software for Windows 7

3. High Performance Video Viewing (Video surveillance cameras and cable future, N. I. C.)
   a. Dell T3500 Precision Workstation
   b. Intel® Quad Core Xeon® W3520 2.66GHz, 8M L3, 4.8GT/s, Turbo
c. 4GB, 1066MHz, DDR3 SDRAM, NECC (4 DIMMS)
d. 16X DVD+/−RW
e. 250GB SATA 3.0Gb/s with NCQ and 8MB DataBurst Cache
f. 10/100/1000 Ethernet Network Port
g. 1 serial port
h. 8 USB 2.0 ports
i. 19 in. Flat LCD Monitor
j. Dual 256MB NVIDIA® Quadro® NVS 295, 4MON, 4DP w/ 4DP to DVI Adapt
k. Internal Chassis Speakers
l. USB Keyboard
m. USB Optical Mouse
n. Surge Suppression Strip
o. Microsoft Windows 7
p. Microsoft SQL Server 2008 Client License
q. SMS Client Software for Windows 7

1.16 COMPONENTS

A. SMS Software Capabilities: Support an unlimited number of card readers, input points, video cameras, intrusion detection points, and relay outputs. The SMS database server shall support an unlimited number of cardholders, visitors, and assets limited only by the available memory on the ISC. The database server shall also support an unlimited number of system events and System Operator transactions in the history file limited only by available hard disk space. Client Workstations shall be limited only by the limitations of the operating system server software. The SMS functions are categorized into nineteen primary “system modules” which shall include:

1. Access Control
   a. One of the SMS's primary purposes shall be to provide access control. The SMS shall be able to make access granted or denied decisions, define access levels, and set timezones and holidays. An input or output linkage feature shall allow linking of monitor zone points to output control points within Intelligent System Controllers (ISCs). The SMS shall support features such as area control (two man control, hard, soft, and timed anti-passback), database segmentation, and timezone or holiday overrides.

2. Alarm Monitoring
   a. The main Alarm Monitoring window shall provide information about the time and location of the alarm, along with its priority. The main Alarm Monitoring window must be able to sort pending and/or insert new alarms based on any of the following attributes: priority, date or time, alarm description, Intelligent System Controller, Card Reader, Input Control Module, asset name, or cardholder. Date or time sorts must be System Operator selectable to be either ascending or descending and must have the option of displaying the seconds of the minute in which the alarm arrived into the SMS. All columns of information in the main Alarm Monitoring window shall be able to be arranged in any order by the System Operator.
   b. The SMS must allow unique emergency instructions to be specified for each type of alarm. It shall also allow for the automatic sending of alphanumeric pages or e-mail messages upon alarm arrival. A real-time graphical system status tree on the screen shall indicate if card readers, alarm panels, digital video recorders, video cameras, intrusion detection panels, or Intelligent System Controllers are secured, unsecured, in alarm, or offline. Output control operations must be available to lock, unlock or pulse control points as a standard feature. An automatic cardholder call-up feature shall allow the quick search and display of images in the database. A System Operator journal shall be available to log important daily events. A trace function shall be available for System Operators to locate and track activity on
specific cardholders, assets, video cameras, or card readers. An image comparison feature must be provided for use in conjunction with a CCTV interface. All alarms and hardware icons MUST have the ability to control the associated hardware via right-mouse clicks.

c. The SMS must provide the option to be used as a UL 1981 Classified Central Station Automation System. This option must be classified by Underwriters Laboratories for use as a Commercial Burg Central Station Automation System, to allow the monitoring station where it is used to be made compliant with the UL 1981 standard and listed by UL. This classification shall apply to alarm panels monitored through a connected, UL approved Central Station Alarm Receiver.

3. Credential Management
a. The SMS shall include a seamlessly integrated credential management module. The credential management functionality must allow the enrollment of cardholders into the database, capturing of images, biometric data, and signatures, as well as the import or export of employee data. This functionality shall also allow the System Operator to assign and/or modify the access rights of a cardholder.

b. The SMS shall include a seamlessly integrated state-of-the-art, 32-bit, credential creation and production system. This shall allow for the creation of different badge types based on a database field, the linking of that field to a badge type to automate the process of credential production, and the use of security colors, chromakey, and ghosting, to allow officers to quickly identify personnel access authority.

c. The SMS shall have capabilities for biometric verification. Through the enrollment and comparison of hand geometry (the size and shape of an individual's hand and fingers), or fingerprints, the identity of an individual shall be verified.

d. The SMS shall have the ability to crop and rotate an image automatically based on the orientation of the eyes found in the image. This shall include photographs captured from digital cameras, live cameras, scanned images and imported images.

4. Digital Video Management
a. The SMS shall include a seamlessly integrated digital video management module. It shall support real-time linkage of digital video clips to their associated alarms as well as those from linked devices in the SMS database; Access Control hardware for example. This linkage shall happen automatically as defined by the configuration.

b. System Administrators shall define parameters for video segment creation by specifying pre-alarm and post-alarm durations. The system shall automatically associate alarms from linked hardware with the linked camera's pre- and post-alarm durations.

c. System Administrators shall configure video segments by specifying pre- and post-alarm time marks, then link those defined video segments to specific alarms. Each camera shall be configured to have its own unique set of pre- and post-alarm time marks, video quality settings, and failover recorder. The SMS shall allow for the central administration, monitoring, and archiving of digital video and the associated cameras. The SMS shall have the ability to launch video on alarm.

d. The SMS shall support the ability to define video behavior by alarm type. The SMS will dynamically apply the behavior in real-time as alarms come in.

e. The SMS shall support Digital Video Recorders from multiple manufacturers. The SMS shall also support IP-based digital cameras and digital video encoders or servers from multiple manufacturers for advanced video surveillance. The SMS shall support MJPEG, MPEG4 simple profile encoding standards and frame rates to include both PAL and NTSC respectively at maximum of 25/30 frames per second. In addition, the SMS shall support a network-based digital video recorder.

5. Intrusion Detection Management
a. The Intrusion Detection Management System shall provide advanced, seamless integration with Intrusion Detection Panels from BOSCH (D9412 and D7412), Detection Systems (7400xi and 7400xi 4+), Honeywell (Galaxy 8, 18, 60, 128, 500, 504, 512, Galaxy Dimension GD48, Galaxy Dimension GD520), Lenel NGP, and Guardall PX, QX, RX, allowing customers to monitor intrusion detection alarms inside the SMS Alarm Monitoring application, in addition to giving CUSTOMER command and control of supported intrusion detection devices (such as arming and disarming an area). Once alarms are brought into the SMS, they shall be linked to digital video, global I/O activity can be triggered, and they shall be stored in the SMS audit trail. In addition, System Operators shall monitor the status of intrusion detection devices from the SMS Alarm Monitoring Workstation.

6. Asset Management
a. The SMS shall include a seamlessly integrated asset management module to include real time management and tracking of CUSTOMER assets. The SMS shall allow for the centralized management of assets. System Administrators shall be able to generate reports on current asset assignments as well as the history of cardholder assignments for assets. The SMS shall also be able to restrict assets from passing through checkpoints with unauthorized personnel and report assets that pass through checkpoints with authorized personnel. The SMS shall also allow specified readers to require an authorized asset before granting access.

7. Visitor Management
a. The SMS shall include a visitor management module. The visitor management module shall be an application utilizing technology that allows a CUSTOMER to enroll and track visitors of the organization.
b. The visitor management module shall allow a CUSTOMER to enroll visitors, sign them in or out, capture a photo, and capture a driver's license or passport. The visitor management module shall allow System Operators to enter and pre-schedule visits. The visitor management module shall allow System Operators to print visitor badges.

8. Remote Access Level Management
a. The SMS shall include a seamlessly integrated remote access level management module. The remote access level module shall be a desktop-based application technology that allows CUSTOMER managers to assign and remove access levels to and from cardholders in the existing SMS database. All transactions relating to the adding and/or removal of access levels shall be recorded complete with a time and date stamp and the System Operator who made the change.

9. Third-Party Interfaces
a. The SMS shall integrate with a number of third-party hardware and software products. The SMS shall provide an industry standard OPC Server utility to allow the export of any and all SMS alarms and events to industry standard OPC Clients, such as building automation and/or process control systems. The SMS shall also provide the ability for an Alarm Monitoring Workstation to function as an OPC Client that shall accept alarms and events from industry standard OPC Servers, such as those from Building Automation or Process Control Systems.
b. The SMS shall provide seamless integration with fire alarm systems such as Pyrotronics and Notifier, personal safety systems such as Visonic Spider Alert, intercom systems such as Zenitel Alphacom or AlphaNet, and central station alarm receivers such as BOSCH 6500 or 6600 and Osborne Hoffman 2020. The SMS shall allow alarms and events from the third-party systems to report into the same main Alarm Monitoring window as access control alarms. Third-party interface hardware shall be configured in the SMS access control module. In some cases, System Operators shall be able to control third-party hardware devices from the Alarm Monitoring Workstation. Third-party hardware alarms and events shall be stored in the SMS database for audit trail and reporting purposes.

10. System Administration
a. System Administrative tasks such as defining client workstation and System Operator permissions set-up, access groups, timezones, reports, maps, etc. shall be provided from any client workstation on the network. Initial setup of the cardholder screen layout shall occur on the database server. The SMS shall support the use of strong passwords.

11. Mobile Enterprise Solutions
   a. The SMS shall support a Mobile Enterprise Architecture for customers with mobile computing needs. Mobile Enterprise functionality shall be a seamlessly integrated, robust solution that transports virtually all SMS client functions to a wearable, portable computer. The portable computer shall connect to the network and SMS Server via 802.11b wireless Ethernet online, or shall be operated as a standalone solution that synchronizes with the SMS Server on an operational basis.

12. Badge Layout Creation
   a. The SMS shall provide a Badge Layout Creation and Editing Module to allow for the creation of custom badge designs to be created by the CUSTOMER. The SMS shall support credit card, government, and custom credential sizes in either a landscape or portrait format and shall support double sided and edge-to-edge printing.

13. Screen or Forms Creation
   a. The SMS shall provide a Forms Designing and Editing Module that gives System Administrators the ability to modify any standard field to customize any or all of the cardholder, asset, or visitor forms. The SMS shall also allow System Administrators to add custom fields in addition to any standard fields on a minimum of 32 pages each of information for cardholder, visitor, and visit related data. User-defined fields absolutely shall not be pre-defined, meaning only the labels can change while the properties cannot. System Administrators shall have a minimum of 96 pages of which to design their cardholder, visitor, and visit screens with standard and custom fields.

14. Graphical Map Creation
   a. The SMS shall provide Graphical Map Creation and Editing Software that must allow System Administrators to import customized map backgrounds of their facility and to attach custom icons to those maps.

15. Application Programming Interfaces
   a. The SMS shall provide a set of standard Application Programming Interfaces (API’s) and supporting documentation that allows hardware manufacturers and software application developers to integrate their products into the SMS. The Application Programming Interfaces shall allow requests from CUSTOMER to integrate a third-party hardware or software solution based on SMS open architecture and SMS device independence.

16. Data Import
   a. The SMS shall support an import utility that will allow the CUSTOMER or VAR to import cardholder information into the SMS database. This shall allow the CUSTOMER or VAR to pre-populate the SMS database with existing cardholder data and/or add new records to the existing SMS database.

17. Bi-Directional Data Exchange
   a. The SMS shall support a real time, bi-directional data interface to external databases such as Human Resources, Time and Attendance, Food Service Systems. The interface shall allow data to be imported into or exported out of the SMS in real-time or in a batch mode basis. Data used for import shall be retrieved directly from an external database or through an import file. Data provided for export shall be applied directly to an external database or through an export file. Any data shall be imported or exported including image data. The file used for import or created by export shall have the ability to be structured in a wide variety of ways, but shall always be in ASCII text format.
b. The SMS 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 Intelligent System Controller (ISC) database.
   This shall be a guaranteed process, even if the communication path between the
   SMS database server and the ISC 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.

18. API Development Toolkit
   a. The SMS shall allow, through API toolkits, System Administrators to expose
      specific SMS data and events that are relevant to IT information or other third-party
      systems. Conversely, the SMS shall allow, through these same API toolkits,
      System Administrators to accept and process information exposed from the IT
      information or other third-party systems. This shall permit System Administrators to
      develop scripts and applications that allow events in either the IT domain to cause
      appropriate actions in the Security domain, and vice versa.

B. SMS Software Functionality:

1. Timezones:
   a. The SMS shall be capable of creating and storing up to 255 timezones. Each
timezone shall have a minimum of six (6) intervals. Each interval shall be
assignable to any day of the week.
   b. Each timezone shall be assignable to an alphanumeric name of up to 64
characters. Timezones shall be applied to access levels, card reader modes, alarm
inputs, alarm outputs, and alarm masking and logging functions. Timezones shall
be allowed to belong to any or all access levels so that the timezone only has to be
defined once.

2. Access Levels:
   a. Capable of defining a minimum of 32,000 access levels with a minimum of 128
access levels per cardholder per database segment. Access levels shall consist of
a combination of card readers and timezones.
   b. Each access level shall be assignable to an alphanumeric name using up to 64
characters.
   c. Card readers shall have the ability to be assigned to any or all access levels
defined in the SMS. Individual card readers shall be capable of having a distinct
timezone assigned to it.
   d. Allow an ‘Allow User Commands’ option to be assigned on a per access level
basis where keypad readers are in use.
   e. Allow a ‘First Card Unlock’ option to be assigned on a per access level basis.

3. Temporary Access Levels:
   a. Capable of assigning Temporary Access Levels inclusive of the 32,000 assignable
Access Levels.
   b. Each Temporary Access Level shall be assignable to an alphanumeric name using
up to 64 characters.
   c. Each Temporary Access Level shall be definable with a start and end date.
   d. Temporary Access Levels shall be stored in the ISC and functionality shall be
maintained in the event of disconnection with the ISC.

4. Access Groups:
a. The SMS shall be capable of assigning Access Groups with a maximum of 32 Access Levels per Access Group.
b. Each Access Group shall be assignable to an alphanumeric name using up to 64 characters.

5. Precision Access Levels:
   a. The SMS shall be capable of assigning Precision Access Levels in addition to the 32,000 Access Levels with the ability to assign unlimited card reader and timezone combinations.
   b. Each Precision Access Level shall be assignable to an alphanumeric name using up to 64 characters.

6. Holidays:
   a. The SMS shall provide a minimum of 255 Holiday assignments using an embedded calendar. Holidays shall be assigned an alphanumeric name using up to 64 characters and shall be grouped into eight (8) types of holidays, and shall be assignable to individual timezones. Access rights, card reader modes, and alarm masking schedules must be able to be altered when the current date is designated a Holiday.
   b. Dates for Daylight Saving Time changes shall be definable and shall take effect automatically.
   c. The SMS shall support Holiday Ranges that allow a single holiday to span across multiple calendar days.

7. First Card Unlock: Feature that when configured retards a pre-determined timezone activated unlock command until a valid credential has been presented and granted access to the portal.

8. Database Segmentation: Support data segmentation whereby each segment shall have its own set of cardholders, field hardware and system parameters (timezones, access levels etc.). This segmentation shall expand the limitations of the SMS parameters (that is, access levels and timezones) to the maximum capacity of each parameter multiplied by the number of segments. The following list shall be made available for segmentation:
   a. Access Group
   b. Access Levels
   c. Actions
   d. Action Groups
   e. Alarm Inputs
   f. Alarm Mask Groups
   g. Alarm Outputs
   h. Areas
   i. Badge Types
   j. Card Formats
   k. Cardholders
   l. Card Readers
   m. Central Station Receivers
   n. Device Groups
   o. Digital Video Archive Servers
   p. Fire Alarm Panels
   q. Guard Tours
   r. Global I/O Function Lists
   s. Global I/O Links
t. Holidays
u. Intercom Panels
v. Intercom Stations
w. Intrusion Detection Panels
x. ISCs
y. Maps
z. Monitor Zones
aa. Precision Access Groups
bb. Receiver Accounts
c. System Operators
dd. Timezones
e. Tour Groups
ff. Visitors
gg. User Permission Groups

9. Field Hardware Communications:

a. The SMS shall communicate with the ISCs by the following protocols:

1) RS-232
2) RS-485
3) TCP/IP
4) Dialup via Modem

b. Communication baud rate shall be system selectable with a range between 1,200 to 115,200 bits per second.
c. Download communication between the SMS and the ISC shall be fully multi-tasking and shall not interfere with operational functions.
d. Upon loss of communications between the SMS Server and the ISC an alarm shall be created with a time stamp. Upon re-established communication the SMS and the ISC shall automatically re-synchronize from the point of communication loss without operator intervention.

10. Dual Path Field Hardware Communication:

a. Support Dual Path communications between the SMS Server and the ISCs. This shall allow for a redundant communication path in the event the primary path fails. The secondary path shall support all primary path protocols.
b. In the event of a communication failure of the primary path the ISC shall initiate a switch over to the secondary path. During this fail over period the ISC shall periodically check to see if the primary path has been re-established and will automatically switch back upon a successful connection. Alarms shall be generated upon loss or restoration of communications.
c. Indicator displaying the current active path between the SMS Server and the ISC.

11. Multi-Drop Panel Support:

a. Support a multi-drop Intelligent System Controller architecture whereby up to eight (8) ISCs shall be multi-dropped on a single RS-485 communications line and whereby all eight panels communicate back to a single serial communications port.
b. The multi-drop panel support shall be used in conjunction with other ISC wiring support such as the star wiring configuration, home-run wire architecture, and advanced distributed network architecture.

12. Intelligent System Controller Remote Dialup Support:
a. Support Remote Dialup operations to and from the Intelligent System Controller (ISC). The dialup connection shall be either a constant connection or a scheduled connection. If the connection is constant, then every panel shall have its own modem at the host. If the connection is scheduled, then all panels using remote dialup shall have the ability to share the same host modem(s).

b. The LNL-2220 and LNL-3300 shall have native 10/100 Ethernet.

c. System Administrators shall have the ability to define the modems available in the pool. For each modem, System Administrators shall be able to define the modem type and the client workstation that it is installed to.

d. Dialup sessions shall occur under any of the user-defined scenarios:

1) On Demand Connection: A System Operator shall have the ability to automatically initiate a dial in session to an ISC via the Alarm Monitoring application.

2) Scheduled Connection: System Administrators shall have the ability to configure the SMS so that the ISC dials into the SMS at a pre-determined times through use of timezones.

3) Critical Alarm Activated: System Administrators shall have the ability to configure the SMS so that the ISC initiates a dialup session with the SMS when a critical alarm is activated in the field.

4) Buffer Threshold: System Administrators shall have the ability to configure the SMS so that the ISC initiates a dialup session with the SMS when a pre-determined number of events are stored in the ISC memory buffer.

13. SMS to Intelligent System Controller Encryption

a. Data security for encrypted connections between SMS and Intelligent System Controllers shall be provided by the full implementation of the Federal Information Processing Standard, FIPS-197, utilizing the 128-bit Advanced Encryption Standard (AES), also known as Rijandael, a symmetric encryption algorithm. The 128-bit AES encryption MUST be certified by the National Institute of Standards and Technology (NIST). FIPS-197 supersedes the aging Data Encryption Standard (DES) defined in FIPS-46-3. Implementation of FIPS-197 shall solve the data security requirements for open network connections by providing a means to secure the data over the non-secure network by encryption.

b. The Intelligent System Controllers shall also support a 32-bit issue code. This shall only be used when implementing a Physical Access Control Systems (PACS) low and medium security profile enhancement.

14. Intelligent System Controller to Reader Interface and I/O Module Encryption

a. Data security for encrypted connections between Intelligent System Controller and downstream modules (Reader interface and I/O Modules) shall be provided by utilizing the 128-bit Advanced Encryption Standard (AES), also known as Rijandael, a symmetric encryption algorithm.

b. The encryption between the ISC and downstream modules must support use of a diversified session key derived from a shared secret master key algorithm. The shared secret master key must be settable to insure uniqueness, and to authenticate connected modules prior to activating them for the session.

15. Area Control: Provide eight (8) area control features: Global Hard Anti-passback, Global Soft Anti-passback, Timed Anti-passback, Two Person Control, Designated One Person Control, Designated Two Person Control, Tail Gate Control, and Occupancy Limit. Area control shall be a security method of preventing a person from passing their badge to another person for dual entry into a single location utilizing one (1) card.
a. Global Hard Anti-passback Feature: Requires that a badge always be used to enter and exit an area. The controlled areas shall have both entry and exit card readers at all portals. Entry and Exit Readers shall be able to span across multiple ISCs. Areas shall be logically defined under the SMS, and area control shall not be required at all areas of CUSTOMER facility to be utilized. Global Hard Anti-passback shall work in the following manner. A cardholder must present his or her badge at the entry card reader of the area that the person wishes to enter. Once access has been granted into the area, the cardholder cannot present the badge to another entry card reader within the same area without first presenting his or her badge to the respective exit card reader of that area. Should a cardholder attempt to use any other card reader in the same area besides the occupied area’s exit card reader once access has been granted to that area, the cardholder shall be denied access and an alarm shall be reported to the alarm monitoring client workstation. Nested control areas (areas inside areas) shall be definable with a minimum of 64 entry and exit card readers. It shall be possible to have an area within an area and/or multiple areas that are independent of each other in which Global Hard Anti-passback rules shall apply.

b. Global Soft Anti-passback Feature: Requires that a badge be used to enter and exit an area. The controlled areas shall have both entry and exit card readers at all portals. Entry and Exit Readers shall be able to span across multiple ISCs. Areas shall be logically defined under the SMS, and area control shall not be required at all areas of CUSTOMER facility to be utilized. Global Soft Anti-passback shall work in the following manner. A cardholder must present his or her badge at the entry card reader of the area that the person wishes to enter. Once access has been granted into the area, the cardholder cannot present the badge to another entry card reader within the same area without first presenting his or her badge to the respective exit card reader of that area. Should a cardholder attempt to use any other card reader in the same area besides the occupied area’s exit card reader once access has been granted to that area, the cardholder shall be allowed access (if that cardholder has the appropriate access level to access the new area), and an alarm shall be reported to the alarm monitoring client workstation. It shall be possible to have an area within an area and/or multiple areas that are independent of each other.

c. The following summary criteria shall apply under Global Hard or Soft Anti-passback:

1) Initially (Time 0) all cardholders are reset to Area 0.
2) Any cardholder shall enter a controlled area any time after Time 0 by presenting a badge to a SMS entry card reader.
3) A cardholder shall not exit the controlled area unless he or she has entered the area presenting a badge to the SMS entry card reader.
4) A cardholder shall not enter the controlled area a second time unless the cardholder has exited that area previously.
5) A cardholder shall be able to enter through any entry card reader and exit through any exit card reader of a single controlled area.
6) These options shall include a “forgiveness” feature that will allow the System Administrator to reset the anti-passback of all cardholders to Time 0 Area 0, either through a manual override or a timezone command.
7) The SMS shall provide an anti-passback exempt option for privileged or VIP (Very Important Person) cardholders. Cardholders with this option will not have anti-passback rules applied to them.
8) The SMS shall also have a “forgiveness” feature that will allow the System Administrator to assign “one free pass” to an individual cardholder. This shall allow the System Administrator to reset the anti-passback of an individual cardholder to Time 0 Area 0.
d. **Timed Anti-passback Feature:** Permits the System Administrator to decide how long after a cardholder has swiped their badge that they will have to wait before the same badge will be accepted again at the same card reader. This helps prevent multiple swipes by an individual to allow access to others through turnstile doors.

e. **Two Person Control Feature:** Provided to restrict access to certain areas unless there are two (2) cardholders present. This restricts individuals from being alone in restricted or highly secure areas. When an area is configured for Two Person Rule, the following criteria shall prevail:

1) The card reader shall grant access only if two (2) valid cardholders (with authorized access levels) swipe their badges one after the other. In the event that a second authorized card is not presented within 10 seconds of the first authorized badge, the card reader shall reset and the first card will have to be swiped again.

2) Once two (2) people occupy an area, individual access shall be granted.

3) Individual exit shall be permitted until an area is occupied by only two (2) cardholders at which point the Two Person Rule applies for exit.

f. **Designated One Person Control:** The SMS shall allow for a special One Person Mode. This mode shall require that a designated cardholder is present before anyone else is allowed to access a certain area. This restricts individuals from accessing a restricted or highly secure area when not accompanied by the designated cardholder. When an area is configured for One Person Mode, the following criteria shall prevail:

1) The card reader shall grant access only if the designated cardholder (with authorized access level) swipes their badge.

2) Once the designated cardholder occupies an area, individual access shall be granted normally.

3) Individual exit shall be permitted until an area is occupied by only the designated cardholder, once the specific cardholder leaves, the area will again require the specific cardholder to be present before any other individual is allowed to gain access.

g. **Designated Two Person Control:** The SMS shall allow for a special Two Person Rule to restrict access to certain areas unless there are two (2) cardholders present and they are designated a special “Team Member” distinction. This restricts individuals from being alone in restricted or highly secure areas as well as restricting the type of personnel allowed in a certain area. When an area is configured for the Designated Two Person Rule, the following criteria shall prevail:

1) The card reader shall grant access only if two valid cardholders (with authorized access levels and special Team Member distinction) swipe their badges one after the other. In the event that a second authorized card is not presented within 10 seconds of the first authorized badge, the card reader shall reset and the first card will have to be swiped again.

2) Once two (2) people occupy an area, individual access shall only be granted to other cardholders who have been designated the Team Member special distinction.

3) A Second designation, “Supervisor” can be assigned to other cardholders. Cardholders with the Supervisor designation shall be announced by means of a contact closure then their card is presented at the entry reader of the restricted area. The occupants of the restricted area may then choose to grant access to the supervisor by closing an external contact connected to the reader interface module, which will in turn energize the door strike output. Closing this contact at any other time shall not open the door.
4) Individual exits shall be permitted until an area is occupied by only two (2) cardholders with special Team Member distinction at which point the Designated Two Person Rule applies for exit.

h. Tail Gate Control: The SMS shall allow for a tailgate sensor mode. This shall be triggered when a person receives an access granted. Upon receiving an access granted, an output will be fired momentarily, duration must not exceed one (1) second. If two people are granted access, the output shall be fired twice momentarily, duration must not exceed one (1) second. The output shall be configured to auxiliary output one of the reader.

i. Occupancy Limit Feature: Restricts the number of cardholders that shall be present in an area at any given time. The Occupancy Limit area shall be able to be defined by the System Administrator to limit up to 65,000 cardholders to be in that area at any given time. Once the occupancy limit has been reached, a cardholder must swipe out of the exit card reader before the next cardholder may enter. Each area for which Occupancy Limit is enabled shall be definable with up to 64 entry or exit card readers. Multiple Occupancy Limit Areas shall be definable.

16. Interlock group readers
The SMS shall have Interlock support. In the Anti-passback area, there shall be an option to make an area an interlock area. Interlocked areas shall be able to be configured, allowing only one door to be opened at a time within the area. This function shall only be able to be enabled for local anti-passback and shall be unavailable for global anti-passback.

The SMS shall support interlocking group readers. As soon as one door's strike is energized or door is open in the group, all other doors will be denied access until a condition is met. When the SMS USER creates an area with the Interlock set, when one door strike of the area is active or if the door is open, then no door shall be allowed to open and there shall be an alarm.

There shall be an alarm for when access is denied due to interlock reader group. There shall be the alarm, “Interlock Area Busy,” that shall show up when trying to get access from a card. There shall be the alarm, “Exit Request Denied: Interlock Area Busy,” that shall show up when pressing the REX button on the panel. There shall be the alarm, “Cannot Open Door: Interlock Area Busy,” that shall show up when opening a door from the SMS's Alarm Monitoring application. All alarms shall have a priority of 100 in the SMS's System Administration application.

17. Field Hardware Configuration: All field hardware configuration windows shall be accessed from either the SMS Icon Toolbar or from menu options in the menu bar within the SMS configuration module of the software. When a field hardware device is configured, the device shall appear in the graphical system overview tree and in all appropriate forms.

Configuration of Intelligent System Controllers (ISCs), Input Control Modules (ICMs), Output Control Modules (OCMs), and card readers shall be provided in a Windows format and shall include the following features:

a. A tab format to logically group information into a series of forms within an icon or menu option. This shall allow for ease of configuration. For example, all forms that relate to the configuration of card readers shall be grouped together in the ‘Card reader’ icon.

b. Drop-down lists to define features
c. Check boxes
d. Spin buttons
e. Browse Buttons for ease of locating client workstations
f. Sortable Lists
g. Graphical System Overview Tree controls for ease of navigation and use

The SMS shall have the ability for bulk add, modify, and delete privileges for ISCs and card readers to allow for the ease of addition and maintenance of these field hardware devices.
The SMS shall provide the ability to search large lists of devices for a string or substring in the device name.

18. Mustering: The SMS shall support advanced mustering functionality. The mustering function shall provide an automatic capability for registering cardholders that are on site during an incident. Designated exit and entry card readers shall be used to enter and leave hazardous locations and safe locations. When an incident occurs, a Muster Report shall be generated that consists of a listing of all personnel that are within the hazardous locations as well as all personnel that have registered in a safe location.

a. A Hazardous Location shall be defined using entry and exit readers associated with the location. Hazardous Locations shall have both entry and exit card readers at all portals. Hazardous Locations shall require that a badge always be used to enter and exit the area. Entry and exit readers shall be able to span across multiple ISCs. The System shall support nested Hazardous Areas (areas within areas).

b. A Safe Location shall be defined using entry and exit readers associated with the location. Safe Locations shall have both entry and exit card readers at all portals. Safe Locations shall require that a badge always be used to enter and exit an area. Entry and exit readers shall be able to span across multiple ISCs. One or more Safe Locations shall be specified for a given Hazardous Location.

c. A Muster Mode shall mean that an incident has occurred and an evacuation is required of one or more Hazardous Locations. A Hazardous Location shall enter into Muster Mode either automatically via an occurrence of a given hardware event transaction (such as an Alarm Input going active) or manually via a System Operator placing the Hazardous Location into Muster Mode.

When a Hazardous Location goes into Muster Mode, all associated Alarm Monitoring Workstations shall be notified with a breakthrough notification and Muster Reporting shall begin.

d. Muster Reset: A Muster Mode shall be reset by a manual operation that shall mark a given Hazardous Location as no longer in Muster Mode. Depending on the configuration of the Hazardous Location, a Muster Reset shall logically move all personnel recorded in the Safe Locations into another area. This area shall typically be the Hazardous Location itself or the “outside area” in which the Hazardous Exit Readers lead. A Muster Reset shall optionally remove all Badges from all associated Safe Locations.

e. Manual Personnel Movement: The SMS shall allow for System Operators to move one badge, or all badges inside an area, from one area (Hazardous Location or Safe Location) to another.

f. Live Muster Mode Reporting: Upon entering a Muster Mode, a Live Muster Mode Report shall be activated. The Live Muster Report shall be configurable to activate immediately upon entering into Muster Mode, after a specified time period from Muster Mode activation, or after the number of personnel in the Hazardous Location reaches a given count. The Live Muster Report shall be configurable to automatically refresh over time and automatically end once the count of personnel in the Hazardous Location reaches zero.

The Online Muster Status Reporting shall include a current total head count of personnel in the Hazardous Location as well as listing each individual cardholder. An online status indicator in Alarm Monitoring shall show the total number of Cardholders carded into a Hazardous Location and the total number of Cardholders carded into a Safe Location during a Muster Mode. An Alarm Monitoring Workstation that logs on after a Muster Mode has been initiated shall automatically be notified that a Muster Mode is in progress and shall begin displaying a Muster Report according to the reporting configuration.
The Live Hazardous Location and Safe Location Reports shall have the ability to select a Cardholder in the report and bring up their related cardholder record. The Live Muster Report shall display the last location, based on card swipe at a card reader, of each cardholder.

The Live Hazardous Location and Safe Location Reports shall display a summary head count total. The Live Hazardous Location and Safe Location Reports shall be able to be sent to a printer. If there are any Safe Locations associated with the Hazardous Location, the Live Muster Report shall include a split screen Safe Location Report consisting of a report on all associated Safe Locations.

g. Alarm Monitoring: Hazardous Locations and Safe Locations shall be placed on graphical maps as Area Icons. A System Operator shall be able to click onto these icons and either run the Hazardous Locations or Safe Location Report or launch the Live Muster or Safe Location Trace Window. A counter shall be located below the icon to show the total count of personnel in the Hazardous Location or Safe Location.

Hazardous Locations and Safe Locations shall be placed on the System Hardware Status Tree as Area Icons. A System Operator shall be able to click onto these icons and either run the Hazardous Location or Safe Location Report or launch the Live Muster or Safe Location Trace Window. A counter shall be located next to the icon to show the total count of personnel in the Hazardous Location or Safe Location.

19. Alarm Masking Groups: Support a group alarm masking feature whereas System Administrators shall be able to create groups of alarm inputs that enable them to mask or unmask multiple Input Control Module inputs and card reader inputs simultaneously. The following events shall have the ability to be part of an alarm masking group:

   a. Input Control Module Events
      1) Alarm Input Active

   b. Card Reader Events
      1) Auxiliary Input Active
      2) Denied Count Exceeded
      3) Door Contact Tamper
      4) Door Forced Open
      5) Door Held Open
      6) Card Reader Input Tamper

   c. Alarm Masking Groups shall be able to be masked as a group or as individual points.

   d. Alarm Masking Groups must support the ability to be masked multiple times. Alarm Masking Groups shall be able to be masked and/or unmasked via alarm monitoring commands by guards, via card reader keypad function keys, or via global linkage commands.

   e. The SMS shall support "Two Man Control" for masking Alarm Masking Groups.

   f. The SMS shall support an Alarm Masking Group status change (Masked to Unmasked or Unmasked to Masked) action to be linked to a function list that is capable of performing many system actions, such as activating a relay output. The SMS shall support a minimum of 64 Alarm Masking Groups per Intelligent System Controller with a minimum of 200 alarm inputs per Alarm Masking Group.

20. Global Input or Output or Event Linkage:

   a. Support a global linkage feature whereby any input or output or event shall be linked to any other input or output or event in the SMS. Input or Output Linkages shall be able to span across Intelligent System Controllers.
b. System Administrators shall be able to create global I/O function lists, each consisting of a sequence of actions to be performed, such as changing card reader modes, activating outputs, and opening or closing anti-passback areas. Each function list may include up to six (6) actions.

21. Cardholder Escort Control:

a. Support comprehensive escort functionality based upon Access Levels. Access Levels shall include options for “Escort Required,” “An Escort,” and “Not an Escort and does not require an Escort.”

b. Capable of one-to-one and one-to-many Escort to Escorted functionality.

22. Cardholder Use Limits: Support a Cardholder Use Limit feature that shall allow System Administrators to specify the maximum number of times that a cardholder may use their credential at card readers in the SMS.

23. Extended Individual Strike Times: Support Extended Individual Strike Times that allows a card reader’s strike to be active for an extended period of time beyond the pre-determined standard strike time on a per cardholder basis. The extended strike time shall be user-definable up to 255 seconds. Extended strike times shall be set on a card reader by card reader basis.

24. Extended Individual Door Held Open Times: The SMS shall support Extended Individual Door Held Open Times that allows a card reader’s door to be held open for an extended period of time beyond the pre-determined standard held open time on a per cardholder basis. The extended held open time shall be user-definable up to 131,070 seconds. Extended held open times shall be set on a card reader by card reader basis.

25. Extended, on Demand, Door Held Open Times:

a. Support extended, on demand, door held times via a command keypad. The Extended Held Open command configuration shall consist of a command key sequence that shall be from 3 to 6 keys used to enter the number of minutes to extend the door held open time (up to 999 minutes) and a pre alarm time (from 0 to 30 minutes).

b. Only those cardholders having Command Authority at a given card reader configured for ‘Allow User Commands’ shall have the ability to execute the Extended Held Open command at that card reader. The Extended Held Open command shall be available after a valid cardholder has received an Access Grant at the card reader. The cardholder shall have a period of fifteen seconds after the Access Grant to enter the extended held open command sequence.

26. Guard Tour:

a. The SMS shall support Guard Tour functionality. A tour shall consist of one (1) or more checkpoints defined as card readers or alarm inputs that a guard shall check during a guard tour.

b. Each tour shall be assigned a name of up to 128 characters and subsequently assigned to one or more alarm monitoring Workstations that indicate from where automatic tours are to be launched.

c. Each tour shall consist of a series of checkpoints that shall include card readers and/or alarm inputs. Tour checkpoints shall be ordered in the sequence within which they are to be visited. Tour checkpoints shall be assigned minimum and maximum times within which to be reached. A “Tour Beginning” Checkpoint shall also be defined to be linked with output actions. Checkpoints shall be able to be placed onto a graphical map.
d. A tour shall optionally link to live video. Instructional text shall be assigned to a tour. These instructions shall be able to be viewed and printed prior to launching the tour from an alarm monitoring workstation.

e. Tours shall have the option of being scheduled.

f. The SMS shall support random tours.

27. Tour Groups: Tour groups shall be created and assigned a name of up to 128 characters. Tour groups will consist of one (1) or more tours, listed by name.

28. Security Clearance Levels: Security clearance levels shall optionally be created and assigned a name. Security clearance levels shall be assigned to one or more guard tours. A Security Clearance Level is a means of limiting the number of ‘tour guards’ when a tour is launched. Particular Security Clearance Levels shall be assigned only to guards who will need access where the tour will take them. When a tour is launched, only those guards with the security clearance levels shall be listed.

29. Guards: Guards shall be selected from the general cardholder population. Guards shall optionally be assigned one or more security clearance levels. Guards shall be associated with one or more monitoring zones.

30. Scheduling: Tours shall be optionally scheduled. When scheduling a guard tour, a single tour shall be scheduled for a specific time or recurring time. When scheduling a guard tour, a list of tours and tour groups may be associated with a specific time for random selection. Tours shall be assigned a “notification” value in minutes. When a given tour is scheduled for automatic launch, this value shall represent the amount of notice the System Operator is given before the tour is to begin.

31. Tour List: All available tours and tour groups shall be listed within the System Hardware Tree inside of the System Administration module. Tour groups shall be expanded to reveal all tour members.

32. Tour Launching: A tour shall be manually launched or launched based on a pre-defined schedule. For a scheduled tour, the Alarm Monitoring Workstations assigned to that tour shall display a notification X minutes (where X is defined by the System Administrator) prior to the scheduled time. The SMS shall allow the System Operator to manually enter a Badge ID rather than selecting a guard from the list. Upon launching of the tour, a Guard Tour Live Tracking view shall automatically open.

33. Guard Tour Live Tracking Window: Opened automatically at the initiating monitoring station whenever a tour is launched. The Guard Tour Live Tracking Window shall consist of a series of columns including:

a. Checkpoint Sequence Number
b. Checkpoint Name
c. Checkpoint Status
d. Checkpoint Min Time
e. Checkpoint Max Time
f. Checkpoint Time (0 if status is “not reached” or “missed”)
g. The following checkpoint statuses shall be supported:

1) Checkpoint Not Reached
2) Checkpoint Reached On Time
3) Checkpoint Reached Early
4) Checkpoint Overdue
5) Checkpoint Reached Late
6) Checkpoint Out of Sequence
7) Checkpoint Missed
8) Guard Tour Initiated
9) Guard Tour Completed
10) Guard Tour Completed With Errors
11) Guard Tour Cancelled
12) Guard Tour Terminated

34. Random Tours: The SMS shall support random tours.

35. Guard Tour Live Video: Multiple live camera views shall be displayed simultaneously in a "sliding window" format. The next checkpoint to be reached shall be highlighted within the video matrix. The matrix shall include a number of cameras before and after that checkpoint.

36. Elevator Control:
   a. The SMS shall provide elevator control using standard access control field hardware that will permit the restriction of cardholder access to certain floors while also allowing general access to other floors. The elevator control feature shall allow, at the elevator, the use of any card reader and all card reader modes used on any other card reader in the SMS. Each elevator card reader shall control access for a minimum of 128 floors.
   b. The SMS shall be able to track which floor was selected by an individual cardholder for auditing and reporting purposes.

37. Graphical System Overview Tree: Displays a graphical representation of all field hardware (including ISCs, fire panels, intrusion detection devices, personal safety devices, intercom systems, and central station alarm receivers), digital video hardware, access levels, timezones, access groups, holidays, and card formats that have been configured in the SMS. System Administrators shall be able to modify a device that is depicted on the graphical system overview tree or see its properties by double-clicking on the icon and the SMS shall bring them to the appropriate form.

38. Pre-Alarm: The SMS shall support a pre-alarm feature at the card reader. The pre-alarm will sound a tone at the card reader prior to the door held open alarm. The pre-alarm setting shall be configurable for up to a maximum of 131,070 seconds (2,184.5 minutes or 36.4 hours).

39. Alarm or Event Logging:
   a. All alarms and events in the SMS shall by default, always be recorded in the database. The SMS shall give System Administrators the ability to select on a timezone basis, the times that they require the SMS to log specific events to the database.
   b. System Administrators shall have the option for Alarm or Events to be set to log or not to log particular alarms or events on any individual reader and or input.

40. Scheduling Utility:
   a. An integral Scheduling Utility shall be provided. The Scheduling Utility shall allow System Administrators to schedule actions to occur on a one-time or a recurring basis. Recurring schedules shall be configured to begin immediately, last indefinitely, or have optional start and end dates.
   b. The Scheduling Utility shall be available from both the System Administration and Alarm Monitoring applications.
   c. The types of actions that shall be schedulable include but are not limited to:
1) Action Group
2) Event Archiving or Purging
3) Arm or Disarm Area
4) Start of Guard Tour
5) Execution of Data Exchange Scripts
6) Activate, Deactivate, Pulse Device Output and Device Output Groups
7) Global Anti-Passback Reset
8) Download Firmware to ISCs and IP Cameras
9) Download Firmware to Lenel Network Video Recorders (LNVR)
10) Download Database to ISCs
11) Execute Function List
12) Mask or Unmask Inputs, Input Groups, Alarm Mask Groups, Door Forced
    Open or Held Open
13) Open Door, Open Door Group
14) Change Reader Mode
15) Automatic Reports
16) Reset Use Limit
17) Move Bulk Badges from an Area
18) Deactivate Badges
19) Logout Visitors
20) Schedule PTZ Presets

d. The Scheduling Utility shall maintain a history log in the database for actions that it executes.

41. Multiple Card Formats: Support an unlimited number of card formats. Magnetic stripe and Wiegand card formats shall be supported. Each ISC shall support a minimum of eight (8) access control card formats and if applicable, eight (8) asset formats. As such, each card reader shall also be able to support a minimum of eight (8) access control card formats. If applicable, asset readers shall be able to support a minimum of eight (8) access control card formats and eight (8) asset management card formats. The SMS shall support any magnetic stripe format that uses card number, facility code, and issue code combinations with a maximum of a nine digit card number and two digit issue code. The SMS shall support any industry standard Wiegand card format.

42. Card Reader Cipher Mode: Support a card reader Cipher Mode that shall allow authorized cardholders to enter their Badge ID by typing it into a card reader keypad, thus emulating the presentation of the credential to the card reader.

43. Denied Access Attempts Counter: Support a denied access attempts count on a per card reader basis. The “Denied Attempts Count” value shall be configurable from 0 to 255. The following access denial types shall cause the current denied count to be incremented:

   a. Unknown PIN entry at a card reader configured as ‘PIN or Card’ mode
   b. Invalid cipher entry at a card reader in Cipher Mode
   c. Invalid PIN entered for a given card at a card reader configured as ‘Card and PIN’ mode
   d. Non-matching biometric presented for a given card at a card reader in biometric verify mode.

44. Card Reader Timezone Overrides:

   a. Allow for the pre-defined default card reader settings to be overridden or temporarily changed on a timezone basis. At the beginning of a selected timezone, the selected card reader’s operational mode shall be modified from its default mode to any one of the following modes: locked, unlocked, facility code, card only,
card or PIN, card and PIN, card and Biometric, card or PIN and biometric, and/or card and PIN and biometric. The aforementioned options shall be available depending on the type of card reader utilized.

b. Each card reader shall have the ability to have multiple timezone setting overrides assigned to them as required by the System Administrator.

45. Online Context-Sensitive Help: Provide online context-sensitive help files to guide System Administrators and System Operators in the configuration and operation of the SMS. The help menu shall be available from any window in the SMS by pressing the F1 function key or clicking on the Help icon in the toolbar. Help windows shall be context-sensitive so System Administrators can move from form to form without leaving the help window. The SMS shall also come with complete online documentation on the product disc.

46. Monitor Zones:

a. The SMS shall provide System Administrators the ability to segment their access control SMS field hardware devices into various zones or areas where alarm monitoring client workstations will monitor. These zones shall be assigned an alphanumeric name using up to 128 characters.

b. The SMS shall allow subset relationship devices (such as card readers or ICMs to Intelligent System Controllers) to be automatically part of the monitoring zone when an ISC is selected AND it shall allow the System Administrator to define which subset devices (card readers, ICMs, etc.) belong to that monitor zone.

c. Updating of monitor zones shall take place in real time and without requiring operators to re-login.

47. Advanced Field Device Control: The SMS shall allow a System Operator to monitor all alarms in their assigned monitor zone, but only be capable of performing field device control actions on specified devices in the assigned monitor zone. The SMS shall allow System Administrators to set permission control for individual devices within a monitoring zone for command override. The list of permissions for control under the monitor permission groups shall include the following:

a. Access modes
b. Open doors
c. Relay and reader outputs
d. Set panel clock
e. Mask alarms and inputs
f. Unmask alarms and inputs
g. Mask alarm mask groups
h. Unmask alarm mask groups
i. Execute function lists
j. Paging
k. E-mail
l. Panel dialup
m. Standalone test mode
n. Download firmware
o. Arm areas
p. Disarm areas
q. Silence area alarms

48. Alarm or Event Routing:

a. The SMS shall be capable of allowing System Administrators to route alarms and events to various alarm monitoring client workstations on the network. The SMS shall allow any alarm or event to be routed to one or multiple client workstations on
the network regardless of where the alarm is generated in the field. Alarms shall be routed to client workstations on a device by device level.

b. The SMS shall be capable of automatic re-routing of an alarm from workstation X to workstation Y if the alarm is not responded to within a user-definable time period.

c. The SMS shall implement network synchronization that in the event alarm or event is routed to multiple client workstations, once the first client workstation ‘grabs’ the alarm, the alarm or event shall be cleared from all other client workstations. As such, alarms that are routed to an alarm monitoring client workstation which does not have a System Operator logged in shall be queued so that all unacknowledged alarms will report to that client workstation once a System Operator has logged into the SMS. Alarms or Events shall be routed based on default settings or timezone control.

49. Text Instructions: Allow for a set of text instructions to be associated with each alarm that arrives into the SMS. The text instruction function shall allow the System Administrator to enter a minimum of 32,000 characters of text for procedures to follow for each alarm that arrives at the alarm monitoring client workstations. Each alarm or event in the SMS shall have its own unique set of text instructions should the System Administrator desire.

50. Customizable Voice Instructions: Allow for a customizable voice instruction to be associated with SMS alarms. The customizable voice instruction feature shall allow the System Administrator to record a voice instruction of unlimited length.

51. Customizable Voice Annunciation: Allow for a customizable voice annunciation to be associated with SMS alarms. The customizable voice annunciation shall allow the System Administrator to record a voice annunciation of unlimited length.

52. Alarm Attributes: The System Administrator shall have the ability to configure how the SMS handles the annunciation of alarms on an individual basis. Each alarm and/or event shall have the option(s) to:

a. Display at one or more alarm monitoring client workstation.
b. Allow higher priority alarms to be displayed on the alarm monitoring client workstation ahead of lower priority alarms.
c. Require the field device, which generated the alarm to be restored to its normal state before the alarm is cleared.
d. Print the alarm to the local event printer.
e. Have a customized voice message announce at the client workstation.
f. Have the alarm breakthrough to the alarm monitoring window should the System Operator be working in another application.
g. Allow System Operators to change the journal entry once the alarm has been acknowledged.
h. Insure that the alarm will not be able to be deleted from the alarm monitoring window upon acknowledgment.
i. Display text and audio instructions outlining the procedures to follow when responding to the alarm.
j. Automatically call-up associated maps.
k. Automatically call up the associated cardholder record.
l. Automatically call up the associated cardholder photo using the video verification function.
m. Require a password to view the alarm.
n. Require a password to acknowledge the alarm.
o. Require acknowledgment to clear.
p. Allow mandatory journal entry upon acknowledgment.
q. Use pre-defined journal entries for alarms.
r. Select the option for journal entry based upon the specific alarm.
s. Send CCTV interface commands to the matrix switcher.
t. Automatically send an e-mail message.
u. Automatically send an alphanumeric page.
v. Have the alarm appear on the alarm monitoring window with a flashing colored coded bar across the alarm for high priority alarms.
w. Have the alarm, when acknowledged, display an alternative flashing color coded bar across the alarm than for the original alarm color.
x. Trigger a function list(s) when the alarm is acknowledged.
y. Require User Logon for Acknowledgment

53. Alarm-Event Mappings: The SMS attributes in Alarm Attributes shall be assignable on a 'global' basis to all devices that share an alarm description. Thus, the 'door forced open' alarm attributes shall apply to any door with a card reader that is forced opened in the SMS. The SMS shall have the capability to assign a unique group of alarm attributes to specific device or alarm combinations to override the global settings for specific case settings. For example, System Administrators may assign a different set of attributes to be applied to a 'door forced open’ at a bank vault or research facility than they would if the front door was forced open. The SMS must include this type of flexibility. Each device or alarm combination shall have the ability to have its own unique attribute set if the System Administrator desires.

54. System Downloads:

a. The SMS shall provide for the downloading of data to the ISCs. Downloads shall load SMS information (timezones, access levels, alarm configurations, etc.) into the ISCs first, followed by cardholder information and card reader configurations.
b. All ISCs on the SMS shall be capable of either full or selective downloads to individual Intelligent System Controllers and bi-directionally so that alarms will still report to their respective alarm monitoring client workstations as cardholder information is being downloaded.
c. A complete database download of 10,000 cardholder records to all ISCs (regardless of the number of ISCs) must be complete within ten (10) minutes.
d. Information on cardholder status, badge status, timezones or access levels shall download in real time as they are added, modified, or deleted from the SMS.

55. Card Reader Options: Include the following options for each reader on the system:

a. Allow User Commands
b. Rename Auxiliary Inputs
c. Rename Auxiliary Outputs
d. Independently Supervise REX and DPS
e. Configure REX and DPS as Normally Open or Normally Closed
f. Deny if Duress
g. Assume Door Used
h. Alarm Masking
i. Activate Outputs
j. Two Card Control
k. Checkpoint
l. Do Not Activate Strike on REX
m. The ability to allow System Administrators to determine on a timezone basis to log or not to log on a card reader by card reader basis:

1) Access Grants
2) Access Denied
3) Card Reader Status Alarms.

n. Allow for user-definable door strike functionality for each card reader in the SMS.
o. Allow for each card reader to be selected as either an 'in' reader, 'out' reader, or 'none' to allow for ease of reporting time and attendance basic 'time in' and 'time out' data.

p. Enforce Use Limit: This option shall enable Card Use Limits at the card reader limiting the number of times that cardholders may use their credential to gain access at the card reader.

q. Alarm Shunt: The SMS shall have the ability to shunt a door contact of separate intrusion detection systems. When the SMS provides an access granted a dedicated auxiliary output shall first trigger and bypass the door contact of the separate intrusion detection system, and then the door locking mechanism shall unlock. Once the door returns to a secure state the door contact of the separate intrusion detection system shall return to its normal state.

r. Supervise Door: Sets the SMS so that the card reader door contact is wired as a supervised input.

s. Relaxed door forced open detection: The SMS shall provide an option that when selected shall allow for the door to be opened for an additional three (3) seconds time period after the request-to-exit sensor has been returned to the normal state.

t. Allow for one (1) or more access points in a specified area to be armed and disarmed directly from the Command Control Keypad.

56. Input Control Module (ICM) Options: Provide the following options for the Input Control Modules:

a. Alarm Masking: The ability to mask the alarm input on a timezone basis.

b. Local Linkage: The ability to locally link outputs with inputs that are attached to the same ICM or Output Control Module (OCM).

c. Activate Output: The ability to activate an output tied to the ICM or OCM on a timezone basis.

d. Activate Output Always: The ability to activate an output always.

e. Configuration of Debounce Times: The ability to control the amount of time that an input state change must remain consistent in order for it to be considered a real change of state.

f. Configuration of Hold Times: When configuring an Alarm Input, a hold time setting shall be settable from 0-15 seconds.

g. Checkpoint: The ability to configure an input as a designated stop on one or more guard tours.

h. Supervised Input: The ability to specify if a specific alarm contact on the ICM is a supervised or unsupervised contact.

57. Entry or Exit Delay: The ability to set up entry or exit delays for inputs that are attached to any ICM, SRI, or DRI. System Administrators shall have three options for entry or exit delay:

a. Non-Latched Entry: When an input activates, the alarm will not be reported until the Entry delay expires. If the input is still active when the entry delay expires, the alarm will be reported. If the input is not active when the entry delay expires, then the alarm will not report.

b. Latched Entry: When an input activates, the alarm will not be reported until the Entry delay expires. If the input is still active when the entry delay expires AND the alarm has NOT BEEN MASKED, the alarm will be reported. If the input has been masked when the entry delay expires, then the alarm will not report.

c. Exit Delay: When an input activates, the alarm will not be reported (operates as if masked) until the Exit delay expires. If the input is still active when the exit delay expires, the alarm will be reported. If the input is not active when the exit delay expires, the alarm will not be reported.

58. Intelligent System Controller Options: System Administrators shall have the ability to group add, modify, and delete Intelligent System Controllers (ISCs) in the SMS. The SMS
shall have a copy command, allowing System Administrators to easily and efficiently add ISCs. The copy command will copy all information configured for an ISC selected and apply those same characteristics to the new ISC being added. System Administrators shall also have the ability mark ISCs as ‘online’ or ‘offline’ depending on whether those panels are online. The SMS shall also prompt the System Administrator if the System Administrator attempts to configure the number of cardholders (and assets, if applicable) that will be downloaded to an ISC to a number greater than that which the ISC’s memory can handle.

59. Basic Integrated Intrusion Functionality: System Administrators shall have the ability to define Alarm Mask Groups for sets of points within an ISC or IDRC. These sets of points can then be treated as an intrusion area. Indication of events from these points can be masked (disarmed) or unmasked (armed) through the Alarm Monitoring application, from a command keypad, and/or from a supported Open Supervised Device Protocol (OSDP) LCD or Keypad device. The SMS shall support Intrusion Mask Groups. The Intrusion Mask Group shall contain intrusion points. These intrusion points shall be individually configured in the SMS. Once intrusion points are assigned to an intrusion mask group it shall be monitored by the SMS to determine the current state of the intrusion mask group. Alarms shall be reported for the intrusion mask group by the SMS based on the current arming mode and state of the intrusion mask group. For each Command Keypad and supported Open Supervised Device Protocol (OSDP) LCD or Keypad device, the System Administrator shall be able to define which Integrated Intrusion commands (Arm or Disarm or Force Arm or View Faulted points) are allowed and whether a credential is required to execute each of them. The System Administrator shall also be able to assign each Integrated Intrusion command to a function key (if supported by the device), and define up to eight 16-character ASCII strings to be continuously scrolled on the device display (if so equipped).

The command keypad or OSDP LCD or Keypad device shall have the option of providing at least the following capabilities:

a. Visual and Audible indication of entry and exit delays
b. Current status of any faulted points in the group
c. Audible and visual indication that an alarm has occurred
d. After an alarm occurs, a list of points faulted during the previous armed period leading up to the alarm
e. When disarmed, an audible chime when programmed point in the group change state

The SMS shall provide support for disabling Intrusion Commands from the SMS’s Alarm Monitoring application. The option shall configure the SMS so that Intrusion Commands may only be performed from the LNL-CK or HID command keypads. This is a requirement for DIACAP certification.

60. Strike Follower

An output for a reader can be overridden so that it is configured to activate and deactivate timed with a door strike. It can be set for a delay time and/or pulse. There shall be a mode called "Strike Follower". The mode shall be optional and mutually exclusive with alarm shunt and tailgate. Strike Follower shall override the auxiliary 1 output and shall allow the output to follow the strike pulse. It shall be configurable with a delay and a pulse time.

The settings shall include:

a. Activation delay
b. Mode: Pulse or Follower
c. Pulse time: When pulse is used, a pulse time can be specified.

61. Support for iCLASS® serial number read and Badge ID lookup using Fargo® DTC400e printer

The Fargo DTC400e printer shall be supported for prox badge number import or iCLASS serial number import. The DTC400e with iCLASS module shall be supported for serial
number import only; the iCLASS badge number shall not be imported. The feature shall allow a customer-provided cross-reference table to be used to read the iCLASS serial number, look up the badge number in the table, and store the badge number in the SMS badge record. Utilizing this workflow shall require significant customer-provided scripting, and the MANUFACTURER’s Professional Engineering Services shall be highly recommended to aid in implementing this workflow.

62. Alarm Monitoring - Alarms Monitored: When the SMS is configured, the System Administrator shall assign a default monitor zone to be monitored. The monitor zone shall include default alarm types with default timezones of which the alarm type will be monitored. These monitor zones will then be assigned to an alarm monitoring client workstation. The SMS shall allow for the monitoring of a combination of one or more ISCs, ICMs, alarm inputs, alarm outputs, and card readers. If applicable, the SMS shall also allow the monitoring of a combination of digital video recorders, video cameras, fire alarm panels, intrusion detection devices, central station alarm receivers, intercom exchanges, intercom stations, and personal safety panels. System Administrators shall have the option to define monitor zones to include all sub devices of an ISC and/or digital video recorders or to choose which sub devices of an ISC and/or digital video recorder belong to that monitor zone. Alarm monitoring client workstations shall be configured to annunciate any or all of the following types of alarms: access granted alarms, access denied alarms, system alarms, emergency alarms, and/or area control alarms.

63. The SMS shall allow for automatic update of the list of hardware devices as they are added, modified or deleted from the SMS. Newly configured devices and changes to existing devices shall be reflected in the hardware list automatically. The SMS shall indicate a deleted device by changing the icon and text associated with the device. Upon the next login, the SMS shall remove the device from the hardware tree.

64. Alarm Annunciation Configuration: The System Administrator shall have the capability to configure how the SMS handles the annunciation of alarms on an individual alarm or event basis. Each alarm and/or event shall have the option(s) to:
   a. Display on the alarm monitoring client workstation.
   b. Allow higher priority alarms to be displayed on the alarm monitoring client workstation ahead of lower priority alarms.
   c. Require the field device that generated the alarm to be restored to its normal state before the alarm shall be cleared from the alarm monitoring window.
   d. Print the alarm to the local event printer.
   e. Have a customized voice message annunciate at the client workstation.
   f. Have the alarm breakthrough to the alarm monitoring window should the System Operator be working on another application on the alarm monitoring client workstation.
   g. Allow System Operators to change the journal entry once the alarm has been acknowledged.
   h. Require that the alarm not be deleted from the alarm monitoring window upon acknowledgment.
   i. Display text and audio instructions outlining the procedures to follow when responding to the alarm.
   j. Automatically call-up associated maps upon arrival.
   k. Automatically call up the associated cardholder record with photo when the alarm displays.
   l. Automatically call up the associated cardholder photo in the video verification function when the alarm displays for comparison to a live video image at the card reader.
   m. Automatically call up live video from a digital CCTV camera to view the area in alarm.
n. Allow the System Operator to control digital CCTV camera functions including pan, tilt, zoom, focus, and iris controls.
o. Require System Operators to enter in a password to view the alarm.
p. Require System Operators to enter in a password to acknowledge the alarm.
q. Require System Operator acknowledgment to clear.
r. Allow mandatory journal entry upon acknowledgment.
s. Have pre-defined “canned” journal entries for alarms in the SMS.
t. Allow non-essential events to be cleared without requiring System Operator journal entry, while other alarms shall require System Operator journal entry.
u. Send CCTV interface commands.
v. Automatically send an e-mail message to one or more e-mail recipients.
w. Automatically send an alphanumeric page to one or more pagers.
x. Have the alarm appear on the alarm monitoring window with a flashing colored bar across it for high priority alarms based on its priority. Each priority in the SMS shall have its own unique color assigned to it. A minimum of 255 colors must be available for assignment to a minimum of 255 priority levels.
y. Have the alarm, when acknowledged, display a different flashing colored bar across the alarm than for the original alarm color. Each acknowledged priority in the SMS shall have its own unique color assigned to it. A minimum of 255 colors must be available for assignment to a minimum of 255 priority levels.
z. Insert and display alarms based on sort order. System Operators can sort on alarms based on alarm priority, time, date, alarm description, card reader, alarm input device, ISC, cardholder, and if applicable, asset scan ID, asset name, intercom station, central station alarm receiver, transmitter, or transmitter input. All sorts MUST be able to be accomplished in one mouse click.
aa. Allow the System Operator to be able to find the location of the alarm by using a graphical map, the real-time graphical system status tree, or an alarm menu. A map call-up feature must be provided that will show the map associated with the alarm.
bb. Have a function list(s) assigned to it that will trigger when the alarm is acknowledged.
c. Require User Logon for Acknowledgment – This feature shall require a user ID and password to be entered when the given alarm is acknowledged. This ID shall be different than the User ID that is currently logged onto the SMS.
dd. Activate an Action Group – This feature shall allow the System Operator to execute an action group, which shall include one or more actions.

65. Alarm Handling: The handling of alarms shall resemble the following steps.
a. The System Operator shall select the alarm or event by any one of the following procedures:
   1) Clicking with the mouse on the system device map icon representing the alarm
   2) Choosing acknowledge from the menu bar
   3) Highlighting the alarm or event in the alarm list by clicking the mouse
   4) Double-clicking on the alarm or event in the alarm list box
b. Any of the above choices shall put the System Operator in the acknowledgment window. The acknowledgment window shall display the time, date, and a user-defined description of the alarm, as well as any emergency procedures. The acknowledgment window shall present the System Operator with the following choices:
   1) Review instructions or procedures to follow for the alarm
   2) Make a journal entry
   3) Acknowledge the alarm
   4) Listen to audio instructions
   5) Print the alarm and instructions to a local printer
   6) Review any previous journal entries for this alarm.
Until the alarm is acknowledged, the alarm shall remain in the Main Alarm Monitoring Window and be counted in the alarm status line.

System Operators shall have the ability to mark an alarm as 'In Progress', meaning that a System Operator has recognized the alarm and is working on a response. When an alarm is marked as 'In Progress', the SMS shall silence any repeating audio notifications on any Alarm Monitoring Workstation in which the alarm was routed and also remove the alarm sprite notification on any graphical maps that may be displaying the alarm. Other System Operators shall be notified that an alarm has been marked as 'In Progress' by an icon next to the alarm in the Main Alarm Monitoring Window.

Control of the associated field hardware device from which the alarm was generated through a right-mouse click operation shall be available. For example, a System Operator can open a door via a card reader alarm. All field hardware device icons on any screen can control the associated field hardware through a right-mouse click operation. A right-mouse click will invoke a menu item with all available control options for that hardware device.

System Operators shall have the ability to delete the alarm from the alarm monitoring window without acknowledging the alarm. This feature is useful when guards are monitoring access grants to track where cardholders are moving throughout the facility, but do not necessarily want to acknowledge the alarm.

The SMS shall provide a text entry field for the System Operator to enter a journal detailing the cause of specified alarms and the actions taken. The journal shall be mandatory for certain alarms or events per the System Administrator's discretion. The journal shall allow System Operators to enter an unlimited amount of notes. Choosing Acknowledge from this window shall clear the alarm indicator and store the alarm information and journal to the database.

Other alarms shall be displayed by the SMS while any alarm is being addressed. If another alarm occurs, the alarm pending counter shall increase by one and the new alarm shall enter into the alarm list box prioritized in a sort order as defined by the System Operator. Up to 255 alarm priorities shall be available.

The SMS shall allow journals to be retrieved, viewed, and edited on screen to provide the System Operator with the ability to complete unfinished journal entries. Journals shall be saved to the database and to a tape during database backups for a permanent record as required by CUSTOMER regulations.

For card reader alarms, the SMS shall allow System Operators to activate, deactivate, or pulse any or all of the card reader outputs configured and associated with the card reader. The System Operators shall also have the ability to mask or unmask each individual card reader door forced open alarms, door held open alarms, and either or both or the auxiliary alarm inputs configured and associated with the card reader.

66. Current Status Indication: The alarm monitoring window shall provide a visual status that displays the current status of all devices in the device tree including child devices downstream from the primary device. Additionally there shall be a numeric display of card readers, ISCs and ICMs that are offline.

67. Pending Alarm Windows: The SMS shall support a Pending Alarm Window in the Alarm Monitoring Workstation. This shall be a separate window from the Main Alarm Monitoring Window that shall be opened at any time to view a list of only pending alarms. The Pending Alarm Window shall be optionally displayed in conjunction with the Main Alarm Monitoring Window. The Pending Alarm Window shall continuously update as new pending alarms are generated and as existing pending alarms are acknowledged or deleted. Pending alarms shall also display in the Main Alarm Monitoring Window. The Pending Alarm Window shall operate and function in the same manner as the Main Alarm Monitoring Window described throughout this document.

68. Device Group Support: Support device grouping for uniform command and control of groups of devices within the system. Four types of homogeneous device groups shall be supported:
a. Card Reader Groups  

b. Input Groups  
c. Relay Output Groups  
d. Video Camera Groups  

69. Color Coding for Alarm Priorities: Display alarms in the active alarm monitoring window with a flashing colored bar across the alarm based upon priority. Acknowledged alarms may be set with alternate color-coding. A minimum of 255 colors must be available for assignment to a minimum of 255 priority levels.  

70. Highlighting of Unacknowledged Alarms: The SMS shall allow for unacknowledged alarms to automatically be displayed in a pop-up window after a user-defined amount of time. The user-defined amount of time shall be set in System Administration.  

71. Pre-Defined “Canned” Alarm Acknowledgment Responses: Have the capability for pre-defined alarm acknowledgment responses for alarms in the SMS. An unlimited number of pre-defined responses shall be able to be configured for each alarm in the SMS.  

72. Cardholder Record Call-up: From the alarm monitoring window, the System Operator must be able to display a cardholder record with the stored cardholder's image. This feature shall be user configurable to be automatic meaning that the Cardholder Window will automatically appear on the Alarm Monitoring client workstation on cardholder activity and will display the current cardholder's information with photo. The Cardholder Window will automatically update with updated cardholder information as additional cardholder activity is generated. This feature shall be provided at all alarm monitoring client workstations to assist the System Operator in determining the access rights of an employee who may have forgotten his or her badge or to verify that the individual presenting the card is the correct individual cardholder. Utilizing a database search via the input of the cardholder's name or other key search field, or by selecting a cardholder record call-up from the main monitoring window on a cardholder alarm, the SMS must access the employee's personnel file, containing pertinent information and the employee's image for identification by the System Operator. The System Operator shall not be required to exit alarm monitoring to view this information and this operation must not restrict the operation of monitoring alarms. In the event of an access denied or access granted card reader alarm signal to the alarm monitoring client workstation, this function shall be available as a menu or mouse selection, based on the alarm event. Data input by the System Operator shall not be required.  

73. Inactive Badge Alarm: The SMS shall provide an alarm, indicating current badge status, if an attempt to gain access is made with a badge that's status is set to any value other than "Active" in the card holder record. Typical inactive badge status values include “Lost” and “Terminated”. Access shall be denied for this attempt. By default, the SMS shall come with this feature disabled, the System Administrator has the ability to enable this functionality.  

74. Request to Exit Event: The SMS shall provide an event when a Request to Exit (REX) is used. By default, the SMS shall come with this feature disabled, the System Administrator has the ability to enable this on a reader by reader basis.  

75. Real-Time, Live Video User Verification: Have the capability to interface with a CCTV system and display a live video image next to a stored cardholder image record. This feature shall be system configurable.  

76. Cardholder Photo Verification: From the alarm monitoring window, the SMS shall optionally display the stored cardholder photo for each credential presented at the user specified reader(s). This function shall allow an operator to verify that the person using the credential matches the stored photo. The system operator shall be able to select from a list of readers. As the cardholder badges through the selected reader their photo shall appear in the Cardholder Verification window. The system operator shall be able to open multiple Cardholder Verification windows to cover multiple readers at the same time. If the Cardholder Verification window is open when the Alarm Monitoring application is
closed then the Cardholder Verification window shall open automatically next time the application is launched.

77. Cardholder, Card Reader, or any Field Hardware Device Trace: From the alarm monitoring window, the System Operator must be able to initiate several traces of cardholders, assets, and/or field hardware devices while monitoring alarms. This information shall be continuously accumulated in the dedicated trace window until the trace is stopped. The trace operations must not interfere with the operation of the alarm monitoring, and be continuous while alarms are monitored. The results of each trace shall be printable on the report printer or displayed on the screen. The traces shall operate independently, such that one trace may stop and start without interfering with another. Trace windows operate independently of each other and the Main Alarm Monitoring Window. Thus, different Alarm Filter sets shall be settable for each alarm window (Main Window and Trace Windows) open in Alarm Monitoring. For example, the Main Alarm Monitoring Window may not monitor Access Grants Events, while one or more of the trace windows are monitoring Access Grants Events. The operator of the SMS’s Alarm Monitoring application shall be able to acknowledge alarms from any alarm view window (even if they are no longer present in the Main Alarm Window). The alarm view windows shall include Main Alarm Monitor, Trace Monitors, Pending Alarms, and Video Verification. The SMS shall allow for individual alarm acknowledgement and fast or group acknowledgement.

The SMS shall support historical traces. Historical traces shall allow System Operators to specify the date and time range that they would like displayed for the particular device that is being traced. For example, a System Operator may perform a historical trace that shows the last seven days activity at a particular card reader. Events are then added in real-time during and after the database has been searched for historical events. Historical traces shall also have the ability to be run against restored (previously archived) data. The SMS shall allow System Operators to filter alarm types from the history trace window. Alarms that shall be filtered from the trace window are access granted alarms, access denied alarms, system alarms, duress alarms, and area control alarms. If applicable, alarms that shall also be filtered are asset alarms, fire alarms, intercom alarms, central station receiver alarms, video clips, and transmitter alarms. The SMS shall allow for a trace on any ISC, ICM, Alarm Input, Credential, Intrusion Detection Device, Monitor Zone, or card reader to be performed. If applicable, the SMS shall allow for a trace on any asset, intercom, or camera to be performed.

78. Single-Click or Double-Click Device Command Execution: The SMS shall support the ability to execute a device command based on either a single-click or double-click on the field device icon in the System Hardware Status Tree or Graphical Map. For example, double-clicking a card reader icon shall pulse open the door for the configured strike time. Whether a single-click or double-click is used to activate the command shall be determined on a System Operator basis.

79. ‘On the Fly’ New Login of System Operators: Allow a System Operator to login over another System Operator who is already logged into the same client workstation. This process shall log the first System Operator off of alarm monitoring and log the new System Operator on, changing any permissions necessary for that System Operator.

80. Auto Exit to Windows 7 or 2008 or 2003 or XP or Vista Login Window: Configurable to automatically exit the Alarm Monitoring application and log the System Operator out of the Windows 7 or 2008 or 2003 or XP or Vista Operating System when a System Operator logs off an alarm monitoring client workstation. The SMS shall then bring the System Operator to the Windows Login Window for the next System Operator to log on.

81. Grant or Deny Popup Window: The SMS shall have the ability to launch a pop-up window when a request for access is made through global input or output activity, such as when an intercom station is linked to a door. Upon activating the intercom, the pop-up window shall be displayed in the Main Alarm Monitoring Window and the System Operator shall then have the ability to issue a grant or a deny for the open door request.
82. Alarm Monitoring – Column Display and Configuration: Allow System Administrators and System Operators to define which columns are displayed in the Main Alarm Monitoring Window and in which order. System Administrators and System Operators shall also be able to determine the column order.

83. Test Mode: Support a Test Mode for Alarm Inputs, Door Forced Open, Access Grants. Tests on Input Device Groups shall be available to verify that all inputs within the group are operational. Upon entering into Test Mode and for the duration of the test, alarms from members of the group shall either be displayed in a separate window or view on test alarm monitoring client workstations or on all Alarm Monitoring client workstations in which the alarms are usually routed. During the test (the duration of the test shall be set by the System Operator), all inputs within the group are manually activated in the field. At the end of the time duration, a report shall be generated flagging any inputs for alarms that were not received. During the Test Mode, all alarm operations carry on as programmed (that is, Global I/O functions, CCTV commands, printer activity, etc.) so that all functions are tested.

84. Manual Control: Provide the System Operator the option to manually control over all output points or input points connected to the SMS. Control points are defined as any door strike, auxiliary card reader output, or any other relay output point of an Output Control Module (OCM).

85. Destination Assurance: Provide the ability to alert the system operator when a cardholder does not reach a required location and present their credential after entering at a designated checkpoint in a designated period of time.

86. CCTV Interface Option: Capable of passing alarm information via a serial RS232 interface with any CCTV Matrix System that utilizes ASCII commands. When the SMS receives an alarm from any monitoring point on the SMS, a minimum of three (3) ASCII control commands of up to 32 characters each relating to that alarm point may be sent to a CCTV matrix switcher per alarm input or card access alarm. The three (3) commands are sent based upon the following condition:

a. Upon arrival of the alarm at the SMS
b. Upon "selecting" or reviewing of the alarm
c. Upon alarm acknowledgment or clearing the alarm

87. Real-Time, Dynamic Graphical Maps:

a. Support graphical maps that display device or group status, function lists and video cameras dynamically in real-time. The maps may be configured to appear on command or when specified alarms are selected for acknowledgment. Map device icons shall have the ability to dynamically change shape and/or color to reflect the current state of the device. The SMS shall indicate if the field hardware is not operating with the most current version of firmware.

b. Support all map formats listed below:

1) Adobe Photoshop (.psd)
2) AutoCAD DXF (.dxf)
3) CALS Raster (.cal)
4) Encapsulated Post Script (.eps)
5) GEM or Ventura (.img)
6) IBM IOCA (.ica)
7) JPEG (.jpg)
8) JIFF (.jif)
9) Kodak Photo-CD (.pcd)
10) Kodak Flashpix (.fpx)
11) LEAD (.cmp)
12) Macintosh PICT (.pct)
13) MacPaint (.mac)
14) Microsoft Paint (.msp)
15) Port Net Graphics (.png)
16) Sun Raster (.ras)
17) Targa (.tga)
18) TIFF (.tif)
19) Windows Metafile (.wmf, .emf)
20) Windows Bitmap (.bmp, .dib)
21) WordPerfect Raster (.wpg)
22) Zsoft PCS or DCX (.pcx, .dcx)

c. Support map hierarchies or maps within maps. There shall be no limit to the
number of maps that shall be nested hierarchically with each other. Multiple maps
may be displayed simultaneously.
d. Support user-defined icons for field hardware devices. The SMS shall also give
System Operators the ability to affect the mode of card readers, open doors, start
a trace on a device, mask or unmask alarm inputs, and activate or deactivate or
pulse an output from the map icons.
e. The graphical maps shall have the ability to be printed to a local printer.

88. Real-Time Graphical System Status Tree and List Window: The SMS shall support a
real-time graphical system status tree or list window that graphically depicts all field
hardware devices that are configured in the SMS. The real-time graphical system status
tree or list window shall list all ISCs, ICMs, alarm inputs, relay outputs, and card readers.
The SMS shall display if the ISCs, alarm input panels, alarm output panels, or RIMs are
not currently operating with the most current version of firmware. If applicable, the
graphical system status tree or list window shall also list all digital video recorders, video
cameras, and intrusion detection devices, zones, and areas. The tree or list window shall
show the real time status of all these devices (online vs. offline, alarms activated,
masking status, etc.).

89. The graphical system status tree or list window shall include three counters:
a. Active Counter- a counter of the number of active points in the Monitoring Zone.
b. Offline Counter - a counter of the number of offline devices in the Monitoring Zone.
c. Masked Counter - a counter of the number of masked points in the Monitoring Zone.

90. System Operators shall be able to display both list window(s) and graphical system
status tree(s). The List Window shall display all hardware devices separately in their own
row in the window. The following columns shall exist in the list window:
a. Device Name
b. ISC or ICM or OCM Name
c. Current Device Status

91. System Operators shall be able to sort any column in ascending or descending order.
System Operators shall also have the ability to choose what types of devices to display in
the graphical system status tree or list window. The following choices shall be available:
a. Include All Devices
b. Include Specified Devices
   1) Active devices
   2) Offline devices
   3) Masked devices
92. A status bar indicator shall identify the current selections for the list window or graphical system status tree. System Operators shall be able to display multiple graphical system status trees and/or list windows on a single Alarm Monitoring Workstation.

93. The SMS shall give System Operators the ability to acknowledge alarms from the real-time graphical system status tree or list window without going back into the Main Alarm Monitoring Window. The SMS shall also allow System Operators to affect the access mode of card readers, open doors, start a trace on a device, mask or unmask alarm inputs, and activate or deactivate or pulse an output from the tree icons. The system hardware status tree or list window shall have the ability to be printed to a local printer. The SMS shall also allow System Operators to launch a video player to view live video at the video camera selected.

94. Function List icons shall be able to be placed onto the System Status Tree and thus, System Operators shall have the ability to control and activate function lists from the tree.

95. Alarm Masking Group icons shall be able to be placed onto the System Status Tree and thus, System Operators shall have the ability to view the status of the alarm masking groups and control the groups from the System Status Tree.

96. Anti-passback area icons shall be able to be placed onto the System Status Tree and thus, System Operators shall have the ability to control area status (open or closed) from the tree.

97. Automatic Credential Deactivation by Lack of Use: Have an automatic credential deactivation function where a cardholder's credential will automatically deactivate after an extended period of inactivity based upon a predetermined time period. The credential status may be reset by authorized System Operators.

98. Alarm Filtering: Have the capability for filtering out alarm types from the alarm monitoring window. Alarms that may be filtered are access granted alarms, access denied alarms, system alarms, duress alarms, and area control alarms. If applicable, fire alarms, asset alarms, intercom alarms, central station receiver alarms, intrusion detection alarms, video event alarms, and transmitter alarms may also be filtered.

99. Manual Override of Card Readers: Support System Operator overrides of card readers from the alarm monitoring window, graphical maps or the real-time system status tree. Also support the ability to manually set a reader back to default mode.

100. Alarm Masking:
   a. Support the masking of alarms to be controlled on a timezone basis or by manual control.
   b. Support the ability to configure inputs to be “Unable to Mask”.

101. Manual Overrides of Alarm Points and Relay Outputs: The SMS shall support System Operator overrides of alarm points and relay outputs configured in the SMS. System Operators shall have the ability to manually mask or unmask an alarm point and/or activate, deactivate, or pulse a relay output from the alarm monitoring window, the graphical maps, or the real-time graphical system status tree.

102. Online Context-Sensitive Help: Provide online context-sensitive help. The help menus shall be available from any window in the SMS by pressing the F1 function key or clicking on the help icon in the toolbar.

103. Sorting Capabilities: Allow System Operators to arrange the way that alarms and/or events in the alarm monitoring window are listed by sorting the alarms and events. Sort criteria shall be based on priority, time or date, ISC, Card Reader, ICM, Input Device, or...
Cardholder. Additionally alarms and events can be sorted based on asset scan ID, asset name, intercom station, intrusion panel, transmitter, or transmitter input.

104. Alarm aggregation: Alarm aggregation is a mechanism of combining several alarms into a single item (group) based on certain criteria. The SMS’s System Administration application shall have an Aggregate option. A user that has permissions to modify alarms shall be able to enable or disable alarms for aggregation. Alarms shall be aggregated in the Main Alarm Monitoring window if the following criteria are met:
   • Alarms are of the same type
   • Alarms are for the same device
   • The aggregation option is enabled for the alarm type

The group of aggregated alarms shall display the number of alarms in the group as a part of the Alarm Description column if the group contains more than one alarm. Additionally, the alarm description shall be displayed using a bold font. All other columns for the group shall display information for the most recent alarm in the group.

The SMS’s Alarm Monitoring application’s operator shall be able to acknowledge or delete a group of aggregated alarms. When acknowledging or deleting a group of aggregated alarms, all alarms in the group shall be acknowledged or deleted. Acknowledge action shall also involve marking in progress. In case of acknowledgment, the progress bar shall be displayed to indicate the progress of the operation.

There shall be a Fast or Group Acknowledge command. If the command is applied to one or more groups of aggregated alarms, all alarms from the selected groups shall be acknowledged or marked in progress depending on what option the user selected.

105. Runaway Detection: Runaway detection is the situation when there is more than a specified number of alarms coming from a given device within a specified time interval. Runaway detection shall be configurable per segment basis in the SMS’s System Administration application. The System Administrator shall be able to configure runaway detection settings. The following system settings shall be available for each segment:

General settings:
   • Detect runaway devices
   • Number of events*
   • Time interval*
   • Log events to the database*

Receiver Accounts settings**:
   • Number of events
   • Time interval

* The setting shall only be available if 'Detect runaway devices' checkbox is selected.
** The settings shall only be available (visible) if UL1981 license is present. In this case, detection of runaway receiver accounts shall be enabled regardless of 'Detect runaway devices' setting, which is UL1981 requirement.

The SMS’s Alarm Monitoring operator shall be able to be notified when a particular device gets into or out of a runaway condition.

Runaway detection shall be performed by the SMS’s Communication Server per device basis as follows:
1. The Communication Server shall monitor devices that belong to segments having runaway detection enabled in System Options.
2. The Communication Server shall use the runaway detection system settings (Number of Events and Time Interval) for the device segment to determine if the device is in runaway situation (condition).
3. A device shall be considered to be in runaway condition if there are at least 'Number of Events' alarms of the same type coming from the device within a 'Time Interval'.

As a device gets into runaway condition, the following actions shall be taken:
1. 'Runaway Device' alarm shall be generated for the device.
2. The device shall be put into runaway state indicated in the SMS's Alarm Monitoring System Tree as a part of the device status text.
3. The Communication Server shall stop sending events to the SMS's Alarm Monitoring stations.
4. The Communication Server shall stop logging events to the database if 'Log events to the database' option is disabled in System Options.

As a device restores from runaway condition, the following actions shall be taken:
1. 'Runaway Device Restored' alarm shall be generated for the device.
2. The device shall be put back into normal state in Alarm Monitoring.
3. The Communication Server shall resume sending events to Alarm Monitoring stations.
4. The Communication Server shall resume logging events to the database if it was disabled.

The SMS's Alarm Monitoring operator shall be able to see only runaway devices in the SMS's System Status Tree. A 'Runaway devices' option shall be in the SMS’s System Status Options dialog. The option shall be part of Specified Devices group. If the option is selected, runaway devices shall be shown in the SMS's System Status Tree; otherwise they shall not be shown.

106. Masking of Successful Command Acknowledgements: The SMS shall support the removal of ‘success acknowledgements’ that are shown in the Main Alarm Monitoring Window after a command has been successfully executed. The SMS shall allow the successful acknowledgements to be removed on a per System Operator basis.

107. Hardware Update Timer: The SMS shall utilize a hardware update timer whereas the System Administrator can set how often system status updates take place. These updates are reflected in the status bar and the real-time graphical system status tree. This frequency shall be defined in one minute increments and shall be changed ‘on the fly’ by System Operators. Immediate changes in hardware status are reflected immediately in the real-time graphical system status tree.

108. Paging Interface Option: Support a paging interface seamlessly integrated within the SMS Alarm Monitoring application. System Operators shall have the ability to manually or automatically send numeric or alphanumeric paging messages on demand regarding any alarm currently displayed in the Main alarm monitoring window. Pages shall have to ability to be sent to multiple pagers if desired. Allow any pager to be accessed through a paging terminal that communicates through the TAP (Telocator Alphanumeric Paging) protocol.

109. E-mail Interface Option: Support an e-mail interface seamlessly integrated within the SMS Alarm Monitoring application. System Operators shall have the ability to manually or automatically send ASCII text e-mail messages from the Alarm Monitoring application on demand regarding any alarm currently displayed in the Main alarm monitoring window. E-mails shall have to ability to be sent to multiple e-mail accounts if desired. Integrate with Microsoft Exchange Server.

110. Personnel Management and Enrollment:
   a. The SMS shall generate and store personnel records, as well as monitor badge or credential use throughout the facility. These credentials shall be fabricated at any of the SMS enrollment and badging client workstations configured based on data and images that are input and captured at the time of enrollment. Credential images are to be digitized using industry standard JPEG image compression, and printed using a high quality and direct card printing process.
   b. Create and Maintain Cardholder Database: A record for each cardholder shall be created in the badging module of the SMS by entering the required data into appropriate data fields. The System Administrator shall be able to define drop-down list box fields for repetitive entered text (for example: Department, Division,
Title, Building Number, etc.). Drop-down list boxes shall allow the System Operator a variety of pre-defined choices for data input. The screen design shall be configurable to allow the entry of data in any format desired. The tab order shall be configurable, and the cardholder ID field of up to 18 digits shall be optionally generated by the SMS from either manual System Operator entry, automatic selection of the next available ID, or by use of the cardholder’s social security number.

c. Once all fields have been entered, the SMS shall store the applicant's record to the SMS database. These records must be stored in a central database. Updating cardholder data shall be possible at any time by any authorized System Operator. The SMS shall have a field that allows System Administrators to view the last date and time that a cardholder’s record has been modified, without running a report. The cardholder form must be user-definable to allow System Administrators to layout the cardholder form.

d. A SMS data import function shall be available to pre-load the SMS with personnel records and industry standard image formats. This import function shall be capable of adding records to the database at any time.

e. The database shall have key fields that are sorted in an index to allow for faster searches. The System Administrator shall be able to designate fields as required and/or unique fields. No record shall be added to the database that does not contain information within the required fields. No record shall be added to the database that contains a duplicate value in a field that was designated as a unique field.

f. Only System Operators with delete privileges (assigned by the System Administrator) shall be able to delete records. Deleting a record shall permanently remove the record from the database (including image files) to free up the disk space for further use.

g. The System Operator shall have the following functions available when enrolling cardholders: choose a badge type, select access levels, enter personal identification numbers (PIN), and/or any other user-defined fields. The SMS shall allow System Administrators the ability to set a default issue code for all first time prints of credentials. The SMS shall also allow System Administrators the ability to auto increment the issue code each time a new Badge is created or to have the System Operator manually enter in a unique issue code each time a new Badge is created. The SMS shall support a minimum of two digits for the cardholder ID issue codes.

h. The SMS shall utilize keyboard or mouse commands that allow System Operators to quickly create a record for any person. The System Administrator shall be able to define drop-down list box fields for the badge type being issued and default values for the other fields based on the badge type.

i. The cardholder form shall also have the option of displaying a cardholder's signature for the record. The cardholder's current Badge information shall also be displayed on the cardholder form complete with Badge ID number, issue code if applicable, activation and deactivation date and time, and the number of times the current badge has been printed.

j. The cardholder form shall also have the ability to display the cardholder’s stored images in one of two ways.
   1) Photo Display - This option displays the optimum quality photo using the JPEG compressed image stored in the SMS database.
   2) No Photo - This option does not show a cardholder photo.

k. The cardholder form shall also display cardholder ‘Last Access’ information. This field will show the last card reader that the cardholder accessed or attempted to access, complete with a time and date stamp.
111. Modify Existing Field Names of SMS Cardholder Form: The SMS shall provide a method of defining basic user-defined fields. It shall allow System Administrators to rename the standard database fields in the cardholder form of the SMS and move the fields to different locations on the form. Additional functionality shall be available in the advanced Forms Designing and Editing Module.

112. Cardholder Active Badges: A cardholder may possess one or many badges at any one time. If a badge is updated or re-issued, the SMS shall guide the System Operator to first change the existing badge’s status to the appropriate classification (de-activate) before a re-issue of the new badge occurs. By utilizing the previously captured image and employee record, the SMS must allow for fast and efficient re-issuance of a badge. As this re-issued badge is printed, the SMS shall update its database to remove access rights from the old badge number and activate the new badge number. Each cardholder record shall offer a user-definable activation and expiration date field. The activation date shall be changed by a System Operator to establish a future activation date. A System Operator shall be able to re-activate a card that has been previously de-activated. When issuing a new badge to a cardholder, System Operators shall be able to assign the pre-existing badge deactivation date and time to the badge instead of the default deactivation date and time for new badges. The deactivation date and time may be assigned on a per badge type basis. A badge form will keep a complete history of every badge that was assigned to the cardholder’s record. The history shall be complete with cardholder badge ID, issue code, badge type, badge status, activation and deactivation dates and times, PIN numbers, embossed numbers, and anti-passback information.

113. Badge status deactivate
All active badges can be configured to change to another badge status when the deactivate date has passed. It is possible to configure this system-wide or per badge type. The badge status shall change 24-48 hours after the deactivate date.

114. Multiple Active Badges: The SMS shall support a user configurable Multiple Active Badge feature. This shall allow cardholders in the System to have up to a user-defined predetermined number of badges active in the SMS at any one time. System Administrators shall have the ability to set the maximum number of active badges allowed in the SMS.

115. Assign Access Levels: At the time a badge is created it shall be possible to have up to 128 access levels assigned to the cardholder’s badge plus any precision access groups. For convenience, the System Administrator must be able to define default access levels to be assigned for given badge types. If a System Operator has proper authorization, cardholder access levels shall be modified. When a badge is created with access rights, or modified, that change shall be downloaded to all ISCs immediately upon completion of the change. Record changes for access rights shall affect only the modified record, and shall not require a download of the entire cardholder database. The access changes shall be downloaded to the field hardware as soon as the employee record change is complete. This badge record download shall not effect field hardware operations. When a badge reaches its deactivation date or time the SMS shall automatically deactivate the access rights associated with the badge. All access rights of a badge shall be eliminated after the expiration date. Should the cardholder become authorized for access again, new access rights shall be applicable to the same badge, and re-issue shall not be required. Should an expired cardholder swipe his badge after his card has
expired, access shall be denied and an “invalid credential” alarm event shall be generated to the alarm monitoring client workstation.

All cardholder information shall be stored for future retrieval or reporting.

An access level form shall show System Operators all access levels configured in the SMS and the associated access levels that are assigned to the cardholder’s current badge. The SMS shall allow the System Operator to double-click the mouse on any access level to view all of the card reader and timezone combinations that are assigned to that access level.

The SMS shall also support access groups, which shall be assigned to cardholders. Access groups will consist of up to thirty two access levels of which shall be viewed by System Operators by clicking on the desired access group.

116. Bulk Assignment or Modification or Deletion of Access Levels: System Administrators or System Operators shall have the option for Bulk Assignment, Modification, and/or Deletion of Access Levels to active badges for a group of cardholders. This feature shall allow System Operators to perform a search of the cardholder database and then apply any additions, modifications, or deletions of access level assignments to all active badges for that group of cardholders.

117. Search Records: The SMS must allow the System Operator to search for records and images using search criteria on any field(s) in the database. The System Operator must be able to enter the search criteria for one or a combination of fields. In addition, partial searches shall be performed. For example, a partial last name search on “Fit” might return “Fitzpatrick,” “Fitzgerald,” or “Zitzerbauch.” Using a partial name or letter shall return every record in the database that contains that information in its last name field. The SMS shall support basic Boolean logic searches (greater than, greater than or equal to, less than, less than or equal to, equal to). For example, a last name Boolean Search “>B<F” will return to the System Operator all records whose last name begins with the letter C, D, and E. These records shall be viewable sequentially using search keys.

The SMS shall allow for the System Administrator the ability to limit the ability of a System Operator to search the database. Thus limiting System Operators, who are using Alarm Monitoring, from searching through records when pulling up the cardholder screen from an event.

In a query with no matching records, the SMS must display a message within three (3) seconds indicating that there is no match for the key field information supplied.

118. Bulk Deletion of Cardholder Records: System Administrators shall have the option to perform Bulk Deletion functions for a group of cardholders. This feature shall allow System Administrators to perform a search against the cardholder database and then delete that group of cardholders.

119. Mobile Badging Operations: Support seamlessly integrated Mobile Badging Operations that allow the SMS cardholder database to be replicated onto an off the shelf laptop computer. The laptop computer shall then have the ability to go to remote sites to enroll cardholders into the SMS and later synchronize the data.

120. Credentials: Support the following credential types and allow for direct Thermal Dye Sublimation printing onto the credential surface.


b. Proximity credentials: Proximity shall be an access control or identification technology that utilizes radio frequency (RF) circuits in microchip form. The microchips are encoded and transmit the encoded information when activated. The proximity card shall be used with its associated proximity card readers. The SMS shall be provided with the following proximity card design options:
1) The proximity card shall be a polycarbonate-based card that cannot be run through direct card printers. This card shall offer a clip slot pre-punched.

2) The proximity card shall be a PVC dual technology card that employs both proximity and magnetic stripe technology. It shall comply with ISO standard for thickness (30 mil). This card shall allow the printing of cardholder record fields including photo directly on the card.

c. Smart Cards – Contact and Contactless:

1) Contact smart cards shall be utilized for access control or identity verification technology. Through use of an embedded memory chip, protected electronic data shall be stored on the smart card. Standard card configuration shall include cardholder, biometric, and access information. Contact cards shall require insertion into a card reader which interrogates the card via physical contacts. When coupled with a smart card reader, the smart card shall have the processing power to serve as an access control device, for use in network security and physical access control. The SMS must possess the ability to integrate with the ActivIdentity Card Management System. This integration must allow the System Operator the ability to personalize contact smart cards during the badge issuance process. The integration also must allow for communication during such events as badge encoding, activation, deactivation, and deletion.

2) Support MIFARE® contactless smart card technology. Contactless smart cards shall be utilized for access control and/or identity verification. MIFARE cards, developed by Philips Semiconductors, shall be presented to a card reader for a transaction to take place using wireless transmissions. They shall be passive devices, requiring no built-in power source. Power shall be supplied from energy generated in the coil of the card being placed within the radio-wave field of the card reader.

3) With MIFARE cards, security shall be handled with challenge and response authentication techniques, data ciphering, and message authentication checks. Uniqueness of cards shall be guaranteed through serial numbers that cannot be altered.

4) Support shall be provided for encoding MIFARE badges with a custom encryption key. This capability will operate in conjunction with readers configured with a matching key, such that these customized credentials will not be recognized by standard MIFARE readers, and standard MIFARE credentials will not be recognized by these customized readers.

5) The SMS shall support GemEasyLink680 and GemEasyAccess332 or GemProx P2 encoders. Using the GemEasyLink680 and GemEasyAccess332 or GemProx P2 encoders the SMS shall be able to support both 1kByte (8kBit) and 4kByte (32kBit) MIFARE smart cards.

6) The SMS shall support the input of a MIFARE serial number during standalone and inline printing. The SMS shall be able to read the serial number of the MIFARE card during the print process and have it automatically populate the badge ID field.

7) The SMS shall support the creation of genuine, licensed HID format MIFARE badges compatible with standard HID MIFARE readers, without the need to order customized readers from HID.
8) Support shall be provided for the encoding of genuine licensed HID Corporate 1000 format, including full HID Corporate 1000 parity structure, to the HID MIFARE formatted credential.

9) The SMS shall support the creation of vendor-independent Open Encoding Standard (OES) MIFARE badges from completely unprogrammed MIFARE cards. The system shall allow OES badges to be secured with a user-defined MIFARE authentication key for reading, and a different user-defined MIFARE authentication key for writing and modification. The encoding shall be compatible with OES-compliant readers from any manufacturer. In addition to the creation of OES badges, the SMS shall be capable of creating OES re-keying cards that will allow the authentication key of OES compliant MIFARE readers to be reprogrammed without vendor assistance.

10) Support DESfire® contact-less smart card technology. Contactless smart cards shall be utilized for access control and/or identity verification. DESFire cards shall be presented to a card reader for a transaction to take place using wireless transmissions. They shall be passive devices, requiring no built-in power source. Power shall be supplied from energy generated in the coil of the card being placed within the radio-wave field of the card reader. With DESFire cards, security shall be handled with challenge and response authentication techniques, data ciphering, and message authentication checks. Uniqueness of cards shall be guaranteed through serial numbers that cannot be altered. The SMS shall support Integrated Engineering SmartID Pro and Phillips Pegoda encoders. Using the encoders the SMS shall be able to support 16k DESFire smart cards.

11) Support HID iCLASS® contactless smart card technology. Contactless smart cards shall be utilized for access control and/or identity verification. iCLASS cards, developed by HID, shall be presented to a card reader for a transaction to take place using wireless transmissions. They shall be passive devices, requiring no built-in power source. Power shall be supplied from energy generated in the coil of the card being placed within the radio-wave field of the card reader.

12) With iCLASS cards, security shall be handled with challenge and response authentication techniques, data ciphering, and message authentication checks. Uniqueness of cards shall be guaranteed through serial numbers that cannot be altered.

13) Support shall be provided for encoding iCLASS badges with a custom encryption key. This capability will operate in conjunction with readers that have been ordered with a matching key, such that these customized credentials will not be recognized by standard iCLASS readers, and standard iCLASS credentials will not be recognized by these customized readers.

14) Support shall be provided for the encoding of genuine licensed HID Corporate 1000 format, including full HID Corporate 1000 parity structure, to the iCLASS credential.

15) The SMS shall support HID OEM-100 and OEM-150 encoders. Using the HID OEM-100 and OEM-150 encoders the SMS shall be able to support 2k and 16k iCLASS smart cards.

16) US Government Smart Cards: The SMS shall support reading the access control data (FASC-N) from US Government issued Contactless smart cards, including PIV end point dual interface cards, as well as compatible cards such as CAC dual interface cards, so long as the cards conform to the requirements outlined in FIPS-201 and HSPD-12.

17) Support shall be provided for reading the 200 bit BCD FASC-N output of FASC-N readers, and concatenating the Agency Code, System Code, and
Credential Code into a full, globally unique 14 character credential number. The concatenated credential number must be the human-readable equivalent of the three fields in a string. Alternative representations are not acceptable.

18) Support shall be provided for reading the 75 bit Wiegand Binary output of GSA approved FASC-N readers, and concatenating the Agency Code, System Code, and Credential Code fields into a full, globally unique 14 character credential number. The concatenated credential number must be the human-readable equivalent of the three fields in a string. Alternative representations are not acceptable.

19) The SMS shall support mapping and importing of the full FASC-N data contained on TWIC (Transportation Worker Identification Credential) and PIV cards. The “Full FASC-N (Hexadecimal)” shall be provided as a field in the FASC-N drop-down in the SMS forms designer tool to map to the full FASC-N data contained on TWIC and PIV cards. TWIC card values shall be mapped to the corresponding cardholder user-defined fields in order to make import possible. A TWIC or PIV import source shall be supported to import the data. If using a TWIC import source, the PIV data shall be imported along with the TWIC Privacy Key and the full FASC-N data. However, if using a PIV import source, only the PIV data shall be imported. A PIN shall be required to import the following PIV data fields: Fingerprints, Facial image, and Printed information. Without a PIN, only these PIV data fields shall be imported: FASC-N, GUID, and Card Expiration Date. The TWIC data shall not require a PIN. It shall be imported into the database for hardware integration use and shall be not visible to the user.

20) The SMS shall support the import of the photograph and fingerprint biometric from the government issued smart card that is compliance with FIPS-201. The SMS shall allow for the verification of the cardholder’s biometric fingerprint against the imported fingerprint. The option of validating the fingerprint and or the import of the biometric shall be configurable SMS wide.

121. Enrollment and Credential Creation - Enrollment:
   a. System Operators shall be able to enroll cardholders on a one by one basis. System Operators will fill in all required fields including name and badge type. The SMS shall determine a number of attributes based on the cardholder’s badge type. These attributes shall be:
      1) Default Deactivation Date or Time - The deactivation date or time shall have the ability to be set for a pre-determined number of days, months, or years; or for an exact specified date.
      2) Default Access Levels
      3) Badge Design Layout
      4) Which Printer will Produce the Badge
      5) Information and Encoding Format to be Encoded onto the Magnetic Stripe

   122. Based on the badge type selected, additional fields shall be required for data entry above and beyond the standard required fields. For example, a Contractor badge may require the field “Company Representing” to be filled in before the badge can be saved and printed.
   a. System Operators shall also enter a Badge ID of up to 18 digits for the cardholder. The cardholder Badge ID shall be determined in one of the following manners:
      1) Manually entered by the System Operator
      2) Automatically generated by the SMS
      3) Use of the Social Security Number as the Badge ID number
      4) Use of EMPI as the Badge ID number
123. Badge ID ranges shall be able to be pre-defined, if desired, by the System Administrator based on Badge Type. For example, the Employee Badge Type may allow Badge IDs to range from 1-49,999 while the Visitor Badge Type Badge IDs range from 50,000-50,999. Multiple Badge ID ranges may be configured for each Badge Type. System Administrators shall have the option of determining how Badge IDs are generated for each Badge Type. For example, the Employee Badge Type shall generate Badge IDs automatically while Visitor Badge IDs must be manually entered into the system at the time of enrollment. Badge ID ranges may be system wide. For example, all Badge IDs (regardless of Badge Type) must fall within a specific range.

124. System Operators shall have the option of utilizing PIN Codes of up to nine digits, embossed numbers, and anti-passback exemptions for each cardholder who is enrolled in the SMS. System Operators shall also assign any temporary access levels for each cardholder that is enrolled.

125. The SMS shall allow for fast and efficient re-assignment of Badge IDs for use for Temporary badges through use of Re-Assignment Wizards. Re-assignment shall be such that the Badge ID shall be stored in the Audit Trail and reported with the cardholder that was assigned to that Badge ID for the specified period of time.

126. Cardholder Image Capture:
   a. Compatible with flash lighting, RGB video cameras, composite input cameras, S-Video input sources, USB sources and digital cameras and allow the capturing of the cardholder image at a minimum resolution of 1024 x 968.
   b. SMS image capture, storage, and hardware compression techniques must be in compliance with the ANSI standard or JPEG (Joint Photographic Experts Group). Cardholder images must be stored as Binary Large Objects (BLOB) within the cardholder record.
   c. Provide the ability to capture a cardholder’s image through the use of any industry standard scanner or digital camera that utilizes a TWAIN interface. Images shall be able to be scanned in at up to 16.7 million colors for a true color scanned image. When using a digital camera that supports multiple resolutions, the system shall allow the operator to select the desired resolution.

127. Image Import: Allow for System Operators to have the ability to import a cardholder’s image at the time of enrollment. The SMS must support the following image formats:
   a. Bitmaps (.bmp, .dib);
   b. JPEG (.jpg);
   c. JFIF (.jif);
   d. Zsoft PCX or DCX (.pcx, .dcx);
   e. Adobe Photoshop (.psd);
   f. CALS Raster (.cal);
   g. GEM or Ventura IMG (.img);
   h. IBM IOCA (.ica);
   i. WordPerfect Raster (.wpg);
   j. Macintosh PICT (.pict);
   k. Portable Network Graphics (.png);
   l. TIFF (.tif);
   m. Windows Metafile (.wmf, .emf);
   n. Targa (.tga);
   o. Kodak Photo CD (.pcd);
   p. Kodak Flashpix (.fpx);
   q. Encapsulated Post Script (.eps).
128. Auto-crop the Enrollment Photograph: The SMS shall allow the image being captured or imported to be automatically cropped based on the location of the eyes in the captured or imported image. The SMS shall also allow the operator to override the auto-crop with a manual crop window.

129. Crop Window Attributes: The SMS shall allow for the image capture crop window to be both movable and sizable. System Administrators shall have the option to give System Operators the ability to size and/or move the crop window. System Administrators shall have the ability to have the SMS maintain the aspect ratio of the image if the captured image is smaller or larger than the pre-defined image object on the badge.

130. Business Card Scanner Enrollment: The SMS shall support an integrated business card scanner for automatic population of specific visitor information fields. The VMS shall support the Corex CardScan business card scanner.

131. ID Scanner Enrollment: The SMS shall support an integrated Driver’s License, passport, government ID, and military ID scanner for automatic population of specific visitor information fields, photo, and signature. The VMS shall support the IDScan CSS-800 and CSS-1000 scanners. The SMS shall support bar code scanning for both scanners.

132. Biometric Verification: Biometric verification shall be available as a seamlessly integrated solution with other SMS modules. Through the measurement and comparison of human characteristics such as fingerprints, hand geometry, or Iris imaging, the SMS shall have the capability to verify the identity of enrolled individuals. The SMS shall NOT require the use of the photo capturing license in order to capture biometrics, the license required for biometric capturing must be separate. The SMS shall NOT require the use of third-party software for enrollment, capture, and encoding of biometrics for the products listed below. These functions shall be seamlessly integrated into the core SMS.

133. The SMS shall provide the ability to view, capture, and delete biometric templates. The System Administrator shall be able to provide permission to view, capture, and delete biometric templates to System Operators. The permission to view, capture, and delete inputted biometric templates shall not be all inclusive. For example, some System Operators may only have the ability to capture biometric templates, while others may have the ability capture biometric templates and delete biometric templates. The System Administrator has the ability to assign the System Operator access to any or all of the aforementioned biometric template abilities.

134. Biometric verification shall be available on a timezone basis per reader. For example, card readers on computer labs shall always use card and biometrics, while card readers at other areas use card only during the day and card and biometrics during off hours.

135. Through seamless integration with Schlage Handkey Series and ID3D-R readers, the SMS shall have the ability to seamlessly capture biometric information (hand geometry) and create biometric templates during the cardholder enrollment process.

136. Biometric seamless verification based on hand geometry shall require the accompaniment of a badge or PIN entry using a reader connected to a Single or Dual Reader Interface Module residing on the same Intelligent System Controller, but physically independent of the Biometric Reader Interface and its devices. In the case of PINs, the integrated RSI keypad shall be used.

137. Through seamless integration with Bioscrypt V-Pass FX and V-Station Series fingerprint readers, the SMS shall have the ability to seamlessly capture biometric information (fingerprint) and create biometric templates during the cardholder enrollment process.

138. Biometric verification based on fingerprint shall require the accompaniment of a badge or PIN entry using a reader connected to a Single or Dual Reader Interface Module residing...
on the same Intelligent System Controller, but physically independent of the Biometric Reader Interface and its devices. In the case of PINs, the integrated keypad of the V-Station may also be used.

139. With use of the Schlumberger Reflex 72 Serial Smart Card reader in combination with the AuthenTec FingerLoc AF-S2 Sensor, the SMS shall seamlessly capture biometric information (fingerprint) and create biometric templates during the cardholder enrollment process.

Through integration with Bioscrypt V-Flex 4G, or V-Station 4G fingerprint readers, the SMS shall have the ability to seamlessly capture biometric information (fingerprint) and create biometric templates during the cardholder enrollment process. The SMS shall support Bioscrypt V-Flex 4G and V-Station 4G for V-Smart (iCLASS/MIFARE) encoding.

Through integration with Bioscrypt V-Flex 4G, or V-Station 4G fingerprint readers, the SMS shall have the ability to verify the identity of the cardholder. The readers shall be able to verify templates that are panel-based and card-based (MIFARE and iCLASS).

140. Through seamless integration with Bioscrypt Solutions V-Smart and V-Station readers, the SMS shall have the ability to verify cardholder identity through iCLASS and/or MIFARE ISO 14443A and 15693 contactless smart card technologies. The SMS shall seamlessly capture biometric information (fingerprint) and create biometric templates during the cardholder enrollment process. Biometric verification based on fingerprint shall require the accompaniment of a smart card using a Bioscrypt reader connected to a Single or Dual Reader Interface Module. The SMS shall also support Bioscrypt two finger capture. Bioscrypt two finger capture shall allow for the capture of a Bioscrypt formatted primary and secondary fingerprint per cardholder. This information shall be encoded on a smart card.

141. Through seamless integration with HID Gen2 SmartID MIFARE reader, the SMS shall have the ability to verify cardholder identity through MIFARE ISO 14443A contactless smart card technology. The SMS shall seamlessly capture biometric information (fingerprint) and create biometric templates during the cardholder enrollment process. Biometric verification based on fingerprint shall require the accompaniment of a MIFARE smart card using an HID Gen2 SmartID reader connected to a Single or Dual Reader Interface Module. The SMS shall also support Bioscrypt two finger capture and encoding for the HID Gen2 SmartID reader. Bioscrypt two-finger capture shall allow for the capture of a Bioscrypt formatted primary and secondary fingerprint per cardholder. This information shall be encoded on a smart card.

142. The SMS shall support configuring Magnetic and Wiegand card formats as duress formats. When the controller detects a duress format, it reports events as duress rather than normal. This setting is different from the Deny-On-Duress PIN setting for readers that accept PIN input. The system ignores the duress format setting during badge encoding.

143. If the reader is capable of reversing bit order, a Wiegand card format can be configured with a reversed bit order format. When the controller detects this format, it reverses the bit order of the incoming data before processing it. The system ignores this setting during badge encoding.

144. The addition of Duress and Reverse Bit Order Card Format capabilities enable the SMS to support Bioscrypt Duress Finger function.
145. The SMS shall allow for duress finger support. Duress finger support shall allow users of Bioscrypt Smartcard readers and/or HID Gen2 SmartID readers to capture a primary and a duress fingerprint, and then to generate an "Access Granted – Duress" event if the duress finger is used. The mechanism for achieving this shall be to define different card formats on the panel for the non-duress card data vs. the duress card data. Both the HID Gen2 SmartID reader and the Bioscrypt reader provide different data when a duress event occurs.

146. When capturing a Bioscrypt fingerprint, the SMS USER shall have a choice between designating a 2nd fingerprint as either "secondary" (normal access with second finger) or "duress" (duress access with second finger). The default mode for the second finger shall be preserved between captures and between sessions, to prevent the need for repetitive selection of the same value.

147. The HID Gen2 SmartID reader, V-Smart MIFARE, and V-Smart iCLASS formats shall properly flag the second Bioscrypt template as either secondary or duress, as indicated in the capture process.

148. Through seamless integration with IRIS ID Scan readers, the SMS shall have the ability to verify cardholder identity through iCLASS contactless smart card technologies. The SMS shall seamlessly capture biometric information (iris) and create biometric templates during the cardholder enrollment process. Biometric verification based on iris shall require the accompaniment of a smart card using an IRIS ID reader connected to a Single or Dual Reader Interface Module.

The SMS shall support configuring an IRIS ID iCAM to use its internal reader as an encoder. The SMS shall support IRIS ID Iris application encoding using the IRIS ID iCAM4100 Internal Encoder. Users may want to remove biometric data for security purposes. The SMS shall be able to be configured so that after a successful encoding of an IRIS ID iris template, the biometric data may be removed.

The SMS shall support encoding IRIS ID Iris Access (iCLASS) using iCAM 4010-H1 internal iCLASS encoder.

149. Through seamless integration with HID bioCLASS fingerprint readers, the SMS shall have the ability to verify cardholder identity through iCLASS contactless smart card technologies. The SMS shall seamlessly capture biometric information (fingerprint) and create biometric templates during the cardholder enrollment process. Biometric verification based on fingerprint shall require the accompaniment of a smart card using a bioCLASS reader connected to a Single or Dual Reader Interface Module. The SMS shall utilize a Sagem-Morpho MSO-300, MSO-350, or MSO-1300 USB capture device to capture fingerprints directly into the primary system database, to be encoded onto bioCLASS badges by the SMS. It is not acceptable for fingerprint capture to be done external to the SMS using a standalone bioCLASS device.

150. Through seamless integration with Cross Match ID-500, Cross Match Verifier 300, or the Sagem-Morpho MSO-300, 350, or 1300, the SMS shall have the ability to capture up to ten fingerprints per enrolled person. This format MUST meet requirements for background checks AND shall also be able to be used with access control systems. The Cross Match ID-500 shall posses a method to recapture all or individual fingerprints depending on the image quality. The Cross Match ID-500 and Verifier 300 shall contain the ability to provide feedback on image quality.
151. All biometric templates shall be stored within the SMS database, and in some cases, the Intelligent System Controller. Additionally, the smart card shall store cardholder, fingerprint, and access information.

a. Seamless Integration

152. Biometrics shall seamlessly integrate with the Access Control and Alarm Monitoring System. Biometric verification alarms shall report in the same Main Alarm Monitoring Window as access control alarms and shall be handled in an identical manner.

153. The same database and network MUST store and transfer information for biometrics and the Access Control and Alarm Monitoring System. A separate database and/or network for the two systems is unacceptable.

154. Biometrics shall seamlessly integrate with the Credential Management System. Biometric information shall be stored in the SMS database along with cardholder information.

155. The same database and network MUST store and transfer information for biometrics and the Credential Management System. A separate database and network for the two systems is unacceptable.

a. Enrollment

156. Biometric templates shall be created during the badge enrollment process or added to existing badges in the SMS database. Biometric information shall also be stored at Intelligent System Controllers, along with badge information. If a smart card is used, cardholder, biometric, and access information shall be added to the smart card.

157. System Operators shall be able to enroll biometrics templates on a one by one basis. System Operators shall fill in all required fields. The biometric data shall be captured via the configured enrollment reader specified.

158. Biometric enrollment readers shall be directly connected to the enrollment workstation. Field hardware connections shall not be required for enrollment readers.

a. Viewing Biometric Templates

159. System Operators shall be able to perform a search of cardholder records to view biometric templates (if there is indeed an image available for viewing) that are currently associated with that cardholder.

160. Federal Agency Smart Credential Number (FASC-N) Standard for Government Badge ID Allocation: The SMS shall support the new Federal Credential Number format scheme and file format specifications for Government Smart Cards and Common Access Cards meeting the requirements of GSC-IS v2.1. This specification facilitates efforts to utilize a single credential in physical access control systems across the Federal Government enterprise. The credential number content shall be based upon the format originally described in the Department of Defense (DOD) Security Equipment Integration Working Group specification 012 (SEIWG-012).

161. PACS Card Holder Unique Identifier Low and Medium Protection Profile Support: The SMS shall support a range of protection profiles that are in association with an extensible data model on Federal Agency Smart Credential (FASC) Cards. The range of protection profiles shall contain the following profiles: low, medium, and high. Using the methods prescribed for each protection profile, a Physical Access Control System (PACS) shall
function for the intended purpose at the adequate level of security warranted by the specific environment and facilitate a cross-agency interoperability across the population of FASC cardholders. The SMS, at a minimum, must provide support for low and medium protection profiles. The low protection profile must most closely emulate the operation of a magnetic stripe card. The medium protection profile shall provide assurance that the card presented was issued by the application holding secret keys, and card was presented to a reader holding symmetric secret keys.

162. Digital Certificate Management: The SMS shall support Digital Certificate Services to enable System Operators to securely obtain digital certificates for smart card cardholders. The SMS shall allow a System Operator to enroll and issue the smart card to each cardholder during enrollment process. This shall allow the issuing of a Smart Card Logon certificate (which provides authentication) or a Smart Card User certificate (which provides authentication plus the capability to secure e-mail) for the purpose of Smart Card Login to PCs. The Digital Certificate shall allow cardholders to log on to a computer with a smart card, instead of needing to type CTRL+ALT+DEL. The SMS shall be able to link a SMS cardholder account to the cardholder’s Active Directory network account.

a. Smart card readers: The SMS shall support any smart card reader(s) that have been tested by the Microsoft Windows Hardware Quality Lab and have obtained the Windows-compatible logo be installed on Windows 2003 or XP computers.

b. Supported smart cards: The SMS shall support the Gemplus GemSAFE and Schlumberger Cryptoflex smart cards included in the default Windows 2003 installation.

c. System Configuration or Network Account Allocation: The SMS shall enforce the allowable number of Network accounts per Cardholder

d. Linking Network Account to Cardholder Accounts: System Administrators shall be able to link an existing Windows Active Directory Account to an SMS cardholder account. Conversely, System Administrators shall be able to unlink an existing Windows Active Directory Account to an SMS cardholder account.

e. Manage Certificates: Through services such as DataConduIT, IT Administrators shall provide facilities to notify IT of events in the SMS that would potentially lead to certificates being revoked or suspended. Thus, SMS Certificate Services provide facilities to manually perform following actions on issued certificates:
1) View certificates. The System Administrator shall be able to view certificates issued to a particular cardholder by SMS.
2) Revoke Certificates.
3) Renew Certificates.
4) View Certificate Audit Trail. Each Certificate Authority shall maintain an audit trail of certificate requests and the certificates that are issued until they expire. The audit trail shall record all certificate transactions including failed requests and all of the information contained in each issued certificate. It also shall provide the information that is required to revoke a certificate and add it to the revocation list. System Administrators shall query the audit trail to locate and view information about any certificate request or any certificate that has been issued by the SMS.

163. Card Management System Support

a. The SMS shall support any smart card reader that has been tested by the Microsoft Windows Hardware Quality Lab and has obtained the Windows-compatible logo to be installed on Windows 2003 or XP Computers.

b. The SMS shall support ActivIdentity Server, and ActivIdentity Client.

c. The SMS shall support issuing of a credential with the self-issuance and local issuance model. For self-issuance the credential will be issued a temporary pass code that will allow the cardholder to login to the ActivIdentity Self Service Portal to
complete the issuance process. For local issuance the credential will be given a permanent pin number to secure the credential. The credential will also be completely personalized with all certificates and applications, based on the configuration of the CMS system.

d. The SMS shall support verifying the cardholder's fingerprint while the card is being issued. This option shall be configurable as a system wide setting.

e. The SMS shall read the card serial number during issuance, either inline during the printing process or on a stand-alone PCSC compliant reader or encoder that is connected to the workstation.

f. The SMS shall support the issuance of a card that either has a pending request from a third-party IDMS (Identity Management Server) or create a new request. The issuance of a card based on a previous request, shall be configured as a system wide setting.

g. The SMS shall support the issuance of a new card and a permanent replacement card. During the issuance of a permanent replacement card the certificates will be transferred to the new card, based on the configuration of the CMS system.

164. Desktop Smart Card Encoding Support: The SMS shall support desktop smart card encoding for the following reader and technologies:
   a. Integrated Engineering (MIFARE)
   b. Bioscrypt V-Smart (iCLASS and MIFARE)
   c. GSC (iCLASS and DESFire)
   d. IRIS ID Access (iCLASS)
   e. HID MIFARE
   f. HID iCLASS Access Control

165. In-line Smart Card Encoding Support: The SMS shall support in-line smart card encoding for the following readers and technologies:
   a. Credential Agent
   b. Integrated Engineering (MIFARE)
   c. Bioscrypt V-Smart (iCLASS and MIFARE)
   d. GSC (iCLASS and DESFire)
   e. IRIS ID Access (iCLASS)
   f. HID MIFARE
   g. HID iCLASS Access Control

166. Badge Design: Support the ability to create and maintain badge designs. Features shall include the ability to support:
   a. Complete Badge design and Layout tools
   b. Chromakey
   c. Image Import
   d. Ghosting
   e. Signature Capture
   f. Bar code
   g. Smart chip support

167. ID Printers: The SMS shall support double-sided full color printing on those printers in which double-sided full color printing is available. The SMS shall also support edge to edge printing on those printers in which edge to edge printing is available. The SMS shall support high-speed printing on those printers in which high speed printing is available. The SMS shall also support holographic overlays on those printers in which holographic overlay support is available.
168. Avery Dennison Badge Label Templates: Provide pre-defined badge layouts that are specific to match Avery Dennison’s US and International self adhesive ID labels.

169. Print Limits: The SMS shall allow System Administrators to limit the number of times a cardholder’s credential can be printed.

170. Intelli-Check ID Check Integration: The SMS shall integrate with the Intelli-Check ID Check 1400 product that allows the scanning of credentials, such as driver’s licenses, military IDs, and government IDs in order to populate the cardholder form during the enrollment process. The Intelli-Check integration shall speed the enrollment process, verify identities and false IDs, and ensure accurate input of information.

171. Batch Printing: The System Operator must be able to print a credential immediately or continue enrolling cardholders with the intention of batch printing at a later time. The SMS Badging client workstation shall have the ability to print a large volume of badges with a single command using a search command. The System Operator must have the option of printing all badges, printing selected badges, or pre-viewing badges without printing. The SMS shall have a ‘log errors’ feature for batch printing. This means that the SMS shall skip any Badges that cannot print due to missing information. For example, in a 200 card batch print job, there may be three cards that require information that is not available because the System Operator failed to enter the information. When printing, the SMS shall skip those three cards and print the other 197. A report can later be run to determine what information is missing for the remaining 3 cards.

172. Print Service Bureau Printing: The SMS shall support the flagging of records to be sent for printing to a print service bureau. The SMS shall only display the option if it is configured and enabled. Once enabled the credentials selected shall be packaged and stored in the SMS database. The packaged records can then be exported and submitted to a print service bureau.

173. In-line Magnetic Stripe Encoding: Utilizing an in-line magnetic stripe encoding device within the printer, the SMS must allow for magnetic stripe encoding of all its permanent credentials. This magnetic stripe shall conform to ABA Track II and ANSI specifications. The SMS shall allow System Administrators to define attributes for card number, facility code and issue code, as well as starting card number. The SMS shall support a multi-track custom encoding feature. System Administrators shall be able to encode user-defined custom expressions on any of the three (3) tracks of the magnetic stripe of a credential. The following information shall be able to be encoded on any of the three tracks of the magnetic stripe:
   a. Access Control Information
      1) Facility Code
      2) Card Number
      3) Issue Code
   b. ASCII Text
   c. Database Fields
   d. ISO or IEC 7812-1 Check Digit

The SMS shall support encoding data onto a JIS II magnetic stripe using JIS II-capable Fargo printers, including the Persona C30, Persona M30, DTC400, DTC550, HDP600, and HDP5000.

174. Image Export: Have the ability to export a captured and cropped cardholder image to an industry standard JPEG (.jpg) file format.

175. Real Time User-definable Image Compression: The SMS must support a real time user-definable image compression utility. The image compression utility shall give System Operators the ability to compare image quality versus compressed image size ratios. This process shall be done in real time and must not require System Operators or System Administrators to go to a program or .ini file outside the program to adjust the ratio. The SMS shall give System Administrators the ability to set SMS default compression settings and give System Operators, with proper permissions, the ability to override those
settings. The better the image quality, the larger the image size (affecting hard drive space and speed of records traveling across the network).

176. Real Time User-definable Video Input Settings: The SMS shall allow for the real time setting of video input devices. User selectable drop-down lists shall be available for RGB, Composite, and S-Video input formats. This process shall be done in real time and should not require System Operators or System Administrators to go to a program or .ini file outside the program to adjust the settings.

177. Signature Capture Window Attributes: The SMS shall allow for the ability to customize the signature capture window so that the window will be more aesthetically pleasing to System Operators. The SMS shall allow System Operators to change the background and foreground colors to a minimum of sixteen different colors for a total of 256 color combinations. The SMS shall also allow System Operators to have the ability to adjust the signature pen pressure to allow for thicker or thinner signatures.

178. Image Processing or Effects Gallery: The SMS shall support cardholder image processing of the cropped captured image through use of a pre-defined image effects gallery. The image processing module shall show both the original captured image side by side next to the processed image. The following effects shall be available to System Operators to apply to an original captured image in any combination desired:
   a. Intensity - Increases or decreases the overall intensity level of the light in the image. Adjusts the brighter areas by making them brighter or darker.
   b. Contrast - Increases or decreases the range of gray levels contained in the image. It adjusts the distinction between the lightest and darkest tones in the image.
   c. Saturation - Adjusts the purity of color (the number of colors used to create a particular color).
   d. Gamma Correct - Enhances detail in the image by adjusting the middle tones without affecting the darkest and lightest areas.
   e. HistoContrast - Adjusts the number of pixels per gray level to create a linear relationship between gray levels, used to bring out the detail in dark areas of the image.
   f. Hue - Adjusts the main characteristic of a particular color that distinguishes it from other colors.
   g. HistoEqualize - Redistributes shades of colors to adjust imbalances. It makes the darkest colors black and the lightest colors white and stretches the colors in-between.
   h. Flip - Flips the image horizontally (the image will appear upside down).
   i. Reverse - Flips the image vertically, creating a mirror image of the original.
   j. Rotate - Rotates the image 0-360 degrees.
   k. Shear - Applies the look of three-dimensionality to the image, while maintaining the original size and shape.
   l. Add Noise - Creates a granular effect that adds texture to a flat or overly blended picture.
   m. Average - Converts each pixel in the image to the average of itself and the pixels to the right and bottom, resulting in a blurring of the image.
   n. Sharpen - Enhances the edges and brings out the detail.
   o. Halftone - Converts the image to a black and white (1 bit/pixel) image in which different shades of gray (luminance) are represented by different patterns of black and white pixels.
   p. Median - Reduces the amount of graininess (noise) in an image.
   q. Emboss - Converts the image to a raised relief style with its light source directed from the top left.
   r. Gray Scale - Represents the image using up to 256 shades of gray.
   s. Invert - Inverts the colors in the image as on a photographic negative.
   t. Mosaic - Converts the image to a grid of square blocks of color.
   u. Posterize - Reduces the color resolution, which is the number of shades of color that shall be displayed simultaneously.
v. Filleting - Rounds the corners for images within a badge layout.
w. Preserved Aspect Ratio - Preserves the aspect ratio of images within badge layouts so that the object rectangle is always filled.

The SMS shall allow for the System Operator to save any combination of effects as a profile to be used on other original images for image processing. These profiles shall be used in conjunction with the image effects gallery. Profiles shall have the ability to be added or deleted from the SMS at any time. The SMS shall ship with a minimum of 6 pre-defined image effects.

The SMS shall support an image effects gallery that shall take the original image and apply up to six pre-defined effect profiles to the image. These profiles shall display side by side in a gallery for the System Operator to select. The System Operators shall have the option of choosing which profiles are applied to the original image in the gallery by selecting from all saved profiles in the drop-down list underneath the processed photo’s image.

179. Bar code Support: Support the following bar codes:

   a. Code 3 of 9 (3:1)
   b. Code 93
   c. UPCA
   d. EAN 13
   e. EAN 8
   f. Code 128 A
   g. Code 128 B
   h. Code 128 C
   i. Codabar
   j. PostNet (Zip +4 Postal)
   k. Code 3 of 9 (2:1)
   l. Interleaved 2 of 5 (2:1)
   m. PDF-417 (2D)
   n. Code 128 Auto
   o. UCC-128
   p. MSI Plessey
   q. Extended Code 3 of 9
   r. Extended Code 93

180. PIV card import: The SMS shall provide the ability to add a contact chip reader to the workstation and to import cardholder information from PIV end point dual interface smart cards (and compatible cards compliant with PIV standards). Imported data shall include at least the following:

   a. FASCN
   b. GUID
   c. DUNS (if it is encoded)
   d. Card Expiration Date
   e. Full Name
   f. First Name
   g. Middle Initial
   h. Last Name
   i. Employee Affiliation
   j. Organizational Affiliation
   k. Agency Card Serial Number
   l. Issuer Identification

181. System Management Console: The SMS shall provide a utility that provides system information and access to log files that can be used to aid in troubleshooting SMS issues.

182. System User Feedback Tool: The SMS shall provide a tool to allow the SMS USER the ability to provide feedback from a menu item available in multiple SMS applications. The
tool shall launch a Web feedback form that allows the SMS USER to send feedback about the SMS to the MANUFACTURER.

183. Device Discovery Utility
The SMS shall provide a Device Discovery Utility (UTILITY). The UTILITY shall allow the ability to discover IP cameras, device servers, access controllers, and wireless access points. The UTILITY shall discover devices in the local subnet as well as across the multiple subnets configured on the network.

The UTILITY shall allow searching and discovering IP cameras on a network, specifically for the purpose of identifying the IP cameras' IP addresses. The UTILITY shall be able to search and discover cameras produced by at least six (6) different camera manufacturers.

The UTILITY shall allow the ability to discover Lantronix® device servers, LNL-2210, LNL-2220, and LNL-3300 access controllers, and Lenel ILS wireless access points. The UTILITY shall support the ability to turn on or off discovery based on device types and manufacturer. The UTILITY shall support displaying the devices grouped by Brand, Discovery Service, Device Status, and Device Type. The UTILITY shall support displaying the devices sorted by Brand, Model, Version, Command Status, IP Address and Port, Hardware Address, Discovery Service, and Device Type.

The UTILITY shall support performing functions (depending on the type of device selected) such as Ping Device, Reboot Device, Check for Default Password, Get Version, Launch Device Web Site, Save Credentials, and Change IP Address.

184. Hardware Devices Notes Field
The SMS shall allow users to enter text as notes for the following types of devices: access panels, readers, video recorders, cameras, fire, intercom, personal safety, receivers, intrusion detection, PLC, POS, and SNMP. These notes shall be available from the SMS's Alarm Monitoring application. The Notes field shall be able to hold a maximum of 1999 characters. The Notes field shall not allow more text to be entered than can be saved. The Notes field shall support Unicode characters for SMS Language Packs.

185. System Administration

a. System Configuration
The SMS shall provide system icons and/or menu selections for each function requiring configuration of SMS options or peripherals (client workstations, field hardware, network functions, communications, reports, etc.). Icon tools bars shall be sizable, movable, and removable. Each form must be in a tab format and shall provide point and click mouse functionality using "icons" or drop-down menus to insure configuration is simple. As soon as a function is defined, it shall appear in any other configuration form list that requires that function. The SMS shall support sorting capabilities for multi-column lists. To sort on a multi-column list, the System Operator shall only have to click on the column that is to be sorted.

These forms shall be available only to the System Administrator to make system additions or changes to existing configurations. All SMS configuration options and forms shall be documented in the System Administrator's Manual to assist in the selection of options.

b. Pre-defined Database
System Administrators shall have the option to install a pre-defined database onto their system complete with sample records and configurations. This sample database shall have a configuration that matches that of the VAR demo cases so that VARs can test and troubleshoot the SMS if necessary.

c. System Configuration Setup Wizards
The SMS shall support SMS configuration setup wizards to guide System Administrators through the configuration of the access control module of the system. The setup wizards shall guide System Administrators step by step by asking a series of questions that, when answered, will allow the SMS to automatically configure itself. The setup wizards shall allow for multiple devices to be added in a single command to allow for easy and efficient
SMS software setup. There shall be at minimum, setup wizards for Intelligent System Controllers and Card Readers.

d. Single Sign-on Support
The SMS shall provide support for single sign on capability. Single sign-on shall allow System Administrators or System Operators to authenticate into SMS applications using their Windows domain account.

Sign sign-on shall support the following scenarios:
1) Allow System Administrators or System Operators to interactively run SMS applications without having to enter a username or password. This shall make administration of the SMS easier since maintenance of separate SMS usernames and passwords is not required.
2) Allow SMS API scripts to authenticate. These scripts shall be run using a Windows account allowing a seamless and secure way to authenticate the account and restricting the script to those actions that the user is permitted to perform.

e. Password Privileges
1) The SMS shall allow the System Administrator to configure each client workstation with those applications that may be run on that client workstation. Individual System Operator passwords will further restrict System Operator functions and shall be specific to each System Operator. Specific System Operator restrictions shall include:
   a) Access to screens or functions (for example: alarm monitoring, badge issue)
   2) Specific tasks allowed (for example: modify data, view only)
   3) Alarm Monitoring functions (for example: clear alarms, output control, traces, reports)

If a System Operator is denied access to specific functions, those functions shall not appear (or shall be ghosted) on the System Operator’s client workstation or menu bar while that password is logged in. Passwords shall not print in any report.

System Administrators and Operators shall have the ability to change their password at any time in the SMS by logging into the SMS with their current password and then changing it through menu options.

f. Strong Passwords
The SMS shall support the use of strong passwords.

g. System Operators
The SMS shall support an unlimited number of System Operators at any time. Each System Operator shall be assigned a logon ID and password. Each System Operator shall be assigned permission levels for system administration and configuration functions, Credential Management functions, alarm monitoring functions, digital video management functions, asset management functions, visitor management functions, remote access level management functions, and database field viewing options.

The SMS shall be able to provide information on the date and time a new System Operator was created. The SMS shall also be able to provide information on the date and time the System Operator information was last modified. There shall also be a notes field when entering a new System Operator where information in regards to the System Operator can be stored.

h. System Permissions
Every major feature, function, and cardholder page in the SMS shall be permission protected. Each System Operator shall be assigned permission or no permission to use or view each feature and function in the SMS. Permission groups shall be broken into three categories: System Administration, Credential Management, and Alarm Monitoring.

Every page in the Cardholder Form shall be permission protected. Each System Operator shall be assigned view permissions for each page of information in the Cardholder Form.
Every database field in the SMS shall be permission protected. Each System Operator shall be assigned view or edit permissions for each personnel database field in the SMS.

i. Network Account Management
The SMS shall support a Network Account Management module. The SMS’s Network Account Management Module shall integrate SMS cardholders with external user network accounts. Through linked accounts, System Administrators shall be able to perform a set of administrative tasks in Windows domains from the System Administration Module. The Network Account Management functionality shall also enable System Administrators to create a link between physical access control and logical domains. The SMS shall additionally be combined with the management of cardholders’ digital certificates stored on a smart card.

j. The integration shall provide a number of benefits, including the ability to do the following:
1) Perform administrative functions on Windows user accounts from within the SMS Administration Module.
2) Enable interaction between Physical Access Control Cardholders and Windows logical domains. For example, if badge is lost, a designated Windows account shall disable.
3) Control access to Computer Anti-Passback Areas
4) Issue Windows 2008 or 2003 Smart Card Logon and Smart Card User certificates on the user’s smart card.
5) Add a New Account

During creation of cardholder records, System Operators shall select an option to create a network account for a new cardholder. The selected network account type shall determine the Windows 2008 or 2003 domain and a set of permissions for the new account.

6) Lost Badge
If a cardholder loses their badge, the System Operator shall change the reported badge status from Active to Lost. When the badge status is changed, all of the cardholder’s linked network accounts automatically shall disabled.

7) Computer Anti-Passback Area Access
Customer has set a security policy, which only allows access to computers in designated areas to personnel physically present in these areas. An employee must present a badge to the card reader in order to enter and exit these secure areas.

A cardholder has access levels that allow him to enter secure area A. In addition, he has a network account of type B, which allows him access to computers in area A. When the cardholder gets “access granted” on entry reader of area A, his computer account of type B is enabled. When the cardholder leaves the area his network account becomes disabled.

k. System Operator Activity Logging
The SMS shall provide full System Operator activity tracking of critical keyboard functions. The activity log shall be comprehensive, recording the date and time of the activity, the client workstation at which the activity was performed, the System Operator who performed the activity, the program the activity occurred in, and the function that was performed within it. The SMS shall record any and all changes to the database made by all System Operators.

The SMS shall log all System Operator functions, including System Operator login and System Operator logout; Additions, Changes, and Deletions to Cardholder Management; New Badge, Print Badge, and Update Badge; and other critical database functions.

The SMS shall log changes made to the access control configurations: Changes of access levels, holidays, timezone changes, card readers, and other critical items.

The SMS shall log changes made to the digital video configurations including changes to digital video recorders, cameras, device links, and other critical functions.

The SMS shall log changes made to the asset management configurations including changes to asset readers, assets, asset assignments and other critical functions.
The SMS shall log changes to the visitor management configurations including the enrollment of visitors, assignment of visitors to cardholders, scheduling visits, and other critical functions. The SMS shall log changes to the intrusion detection management configurations including the configuration of areas and zones, arming or disarming areas, and other critical functions. The SMS shall log activity of System Operators performing SMS alarm monitoring; that is, alarms acknowledged, cleared, output control activity, trace, and other functions. The SMS shall permit the System Administrator to define the number of day's worth of activity to keep online before the System Administrator purges the oldest data offline. The activity log will have a field to show the number of total System Operator events that are currently stored in the database. The number of events to keep online shall only be limited by the amount of disk space available on the database server. The SMS shall provide a System Operator activity report to query the above information available in the SMS database. Client workstation, System Operator, date and time, or other selection criteria shall sort the report. On those occasions when historical data shall be needed, the System Operator activity report shall be generated from an archived database as well as from the active SMS database.

m. Alarm or Event Activity Logging
The SMS shall provide full access or alarm or event activity logging. The activity log shall provide comprehensive logging of date and time of the transaction, where the transaction occurred, acknowledgment information, and any System Operator actions. The SMS shall log all access grants, access denies, alarm actives, asset denies, and other critical and non-critical alarms. The SMS shall give System Administrators the ability to choose when to log certain types of alarms. The log shall be broken down into the following categories: Events and Alarm Acknowledgements, User Transactions, and Visits. For each type of alarm, the System Administrator can set how long to keep each group of events. For example, visits may only be kept in the history file for 7 days while User Transactions may be kept for one year.

The activity log will have a field to show the number of total events that are currently stored in the database. The number of events to keep online shall only be limited by the amount of disk space available on the database server. The SMS shall log a minimum of 1,000,000 events before the System Administrator purges the oldest data to an offline file. The hard drive space required to store 1,000,000 events shall not exceed 40 MB. The SMS shall provide activity reports to query the above information available in the SMS database. The reports shall be sorted by client workstation, alarm type, date and time, or other selection criteria. On those occasions when historical data shall be needed, the activity reports shall be generated from an archived database as well as from the active SMS database.

n. Encryption of PIN Codes inside the Database Server
The SMS shall encrypt all cardholder PIN codes such that no one, including the System's Administrator, shall have access to cardholder PIN codes through the application or through the database server.

n. Access Control Reports
There shall be a minimum of 140 standard SMS reports provided with the SMS. All reports MUST be stored in the SMS database and MUST be able to be viewed from any SMS client workstation with proper permissions. Reports shall use UTC time. The SMS shall allow the SMS USER to e-mail reports based on system events or on a user-defined schedule. The standard reports that shall be included with the SMS are described below:

1) Access Denials and Grants by Reader Report
The Access Denials and Grants by Reader Report shall provide information on all access denials and granted events including time, card reader, badge, and cardholder name, sorted by card reader.
2) Access Denials, Grants, and Other Badge Events Report
The Access Denials, Grants, and Other Badge Events report shall provide information on all badge related events including time, reader, badge, and cardholder name.

3) Access Denied Event Report
The Access Denied Event Report shall provide information on all access denied events including time, card reader, badge, and cardholder name. It shall also include the following events: Interlock Area Busy, Cannot Open Door: Interlock Area Busy, Exit Request Denied: Interlock Area Busy, and DURESS - Interlock Area Busy.

4) Access Denied Events, by Reader
The Access Denied Events, by Reader Report shall provide information on all access denied events including time, card reader, badge, and cardholder name, sorted by card reader. It shall also include the following events: Interlock Area Busy, Cannot Open Door: Interlock Area Busy, Exit Request Denied: Interlock Area Busy, and DURESS - Interlock Area Busy.

5) Access Granted Events Report
The Access Granted Events Report shall provide information on all access granted events including time, card reader, badge, and cardholder name.

6) Access Granted Events by Reader Report
The Access Granted Events by Reader Report shall provide information on all access granted events including time, card reader, badge, and cardholder name, sorted by card reader.

7) Access Groups Report
The Access Groups Report shall provide information on all access groups and the access levels contained in each group.

8) Access Groups with Levels Report
The Access Groups with Levels Report shall provide information on all access group definitions including access level details.

9) Access Level Assignments to Cardholders Report
The Access Level Assignments to Cardholders Report shall list each access level with a listing of each cardholder that has that access level assigned to them.

10) Access Levels Assignment to Cardholders, By Segment Report
The Access Levels Assignment to Cardholders, By Segment Report shall provide information on all cardholders with access levels, sorted by segment. Only personnel with assigned access levels shall be included in the report. This report shall also summarize the total number of badges that will need to be downloaded to each segment. This report only shall only work on a system utilizing database segmentation.

11) Access Levels Report
The Access Levels Report shall provide information on all access level definitions.

12) Access Panels Report
The Access Panels Report shall provide information on all access panel definitions.

13) Active Visits by Cardholder Name Report
The Active Visits by Cardholder Name Report shall provide information on all visits that are currently active (not signed out) grouped by cardholder name.

14) Active Visits by Host Name Report

15) The Active Visits by Host Name Report shall provide information on all visits that are currently active (not signed out) grouped by Host Name.

16) Active Visits by Visitor Name Report
The Active Visits by Visitor Name Report shall provide information on all visits that are currently active (not signed out) grouped by Visitor Name.

17) Alarm Acknowledgments Report
The Alarm Acknowledgments Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes.

18) Alarm Acknowledgements by Definition Report
The Alarm Acknowledgments by Definition Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by Definition.

19) Alarm Acknowledgments by System Operator Report
The Alarm Acknowledgments by System Operator Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by System Operator.

20) Alarm Acknowledgements by Panel Report
The Alarm Acknowledgments by Panel Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by Intelligent System Controller Panel.

21) Alarm Configuration Report
The Alarm Configuration Report shall provide alarm configuration summary information.

22) Alarm Input Events Report
The Alarm Input Events Report shall provide information on all alarm input events sorted by date.

23) Alarm Panel Inputs Report
The Alarm Panel Inputs Report shall provide information on all alarm panel inputs grouped by access panel and alarm panel.

24) Alarm Panel Local Linkage Report
The Alarm Panel Local Linkage Report shall provide information of all input and output linkages within an ICM.

25) Alarm Panel Outputs Report
The Alarm Panel Outputs Report shall provide information on all alarm panel outputs grouped by access panel and alarm panel.

26) Alarm Panels Report
The Alarm Panels Report shall provide information on all alarm panel definitions grouped by access panel.

27) All Cardholders with Logical Access Report
28) The All Cardholders with Logical Access Report shall list all cardholders that have linked accounts through logical access.

29) All Events Over Time Report
The All Events Over Time Report shall provide a listing of all event types over time.

30) All Events Over Time with Local Panel Time Report
31) The All Events Over Time with Local Panel Time Report shall provide a listing of all event types over time. This report also shows the time an event occurred in the panel's time.

32) All Events Over Time with Unique Alarm ID Report
The All Events Over Time with Unique Alarm ID Report shall provide a listing of all event types with an unique alarm ID over time.

33) Anti-Passback Events Report
The Anti-Passback Events Report shall provide a listing of all anti-passback events over time

34) Area Anti-Passback Configuration Report
The Area Anti-Passback Configuration Report shall provide a listing of all anti-passback areas, including the reader entrances and exits.

35) Area Configuration Report
36) The Area Configuration Report shall list all areas, including the reader entrances and exits.

37) Area Entrance History Report
The Area Entrance History Report shall provide a history of all cardholders enter anti-passback areas, sorted by area and date.

38) Asset Classes Report
The Asset Classes Report shall provide information on all asset classes and the asset groups to which they belong.
39) Asset Events Report
The Asset Events Report shall provide information on all asset events.

40) Asset Groups Report
The Asset Groups Report shall provide information on all asset groups and the classes they contain.

41) Asset Types Report
The Asset Types Report shall provide information on all asset types defined with all associated subtypes.

42) Assets by Scan ID Report
The Assets by Scan ID Report shall provide information on all assets grouped by Scan ID.

43) Assets by Type Report
The Assets by Type Report shall provide information on all assets grouped by asset type and subtype.

44) Assigned Assets by Cardholder Report
The Assigned Assets by Cardholder Report shall provide information on all currently assigned assets grouped by cardholder.

45) Assigned Assets by Scan ID Report
The Assigned Assets by Scan ID Report shall provide information on all currently assigned assets grouped by Scan ID.

46) Assigned Assets by Type, Scan ID Report
The Assigned Assets by Type, Scan ID Report shall provide information on all currently assigned assets grouped by type and Scan ID.

47) Audio Notifications and Instructions Report
The Audio Notifications and Instructions Report shall list all audio notifications and instructions in the database.

48) Badge Type Configuration
The Badge Type Report shall provide a listing of all Badge Types.

49) Badges by Deactivation Date Report
The Badges by Deactivation Date Report shall list all badges by deactivation date. Shall be used to determine which badges are about to deactivate.

50) Badges Without Access Levels Report
The Badges Without Access Levels Report shall provide information on all Badges that do not have any access levels assigned to them. Badges with access levels assigned to them shall not be listed in this report.

51) Card Formats Report
The Card Formats Reports shall provide information on definitions of all Magnetic and Wiegand card formats in the SMS.

52) Cardholders Access to Readers Report
The Cardholders Access to Readers Report shall provide a listing of each card reader along with which cardholders have access to that card reader. Includes associated access level and timezone.

53) Cardholder Exit or Entry Report
The Cardholder Exit or Entry Report shall provide information on all user-defined Exit or Entry information on a per cardholder basis. It shall list the time a cardholder swipes their badge at a designated ‘In’ reader and the time they swiped their badge at the corresponding designated ‘Exit’ reader.

54) Cardholder Photo Gallery Report
The Cardholder Photo Gallery Report shall provide cardholder names and photos, sorted by last name.

55) Cardholder Time and Attendance Report
The Cardholder Time and Attendance Report shall pair each in-time with an out-time for cardholders gaining entry to time and attendance readers.

56) Cardholders by Badge Type Report
The Cardholders by Badge Type Report shall provide information on all cardholders sorted by badge type. No access levels are shown in this report and cardholders that have not been assigned a badge type will not be reported.

58) Cardholders by Last Name Report
The Cardholders by Last Name Report shall provide information on all cardholders sorted by last name, with badges but not access levels. Only personnel with badges assigned shall be included in this report.

59) Cardholders Located in Each APB Area by Date Report
The Cardholders Located in Each APB Area by Date Report shall provide a list of all cardholders located in each anti-passback area, sorted by area and date.

60) Cardholders Located in Each APB Area by Name Report
The Cardholders Located in Each APB Area by Name Report shall provide a list of all cardholders located in each anti-passback area, sorted by area and cardholder name.

61) Cardholders with Access, by Badge Type Report
The Cardholders with Access, by Badge Type Report shall provide information on all cardholders with access and precision access levels, sorted by badge type. Only personnel with active badges and access levels shall be included in this report.

62) Cardholders with Access by Last Name Report
The Cardholders with Access by Last Name Report shall provide information on all cardholders with access and precision access levels, sorted by last name. Only personnel with active badges and access levels shall be included in this report.

63) CCTV Instructions Report
The CCTV Instructions Report shall provide summary information on all CCTV instructions in the database.

64) Continuous Video Report
The Continuous Video Report shall provide a listing of all of the times continuous video is archived.

65) Current Visits Report
The Current Visits Report shall provide a list of all currently signed in visits.

66) Destination Assurance Configuration Report
The Destination Assurance Configuration Report shall provide a listing of all card readers configured for Destination Assurance with their associated lead times to proceed to the next defined card reader.

67) Destination Assurance Exempt Cardholders Report
The Destination Assurance Exempt Cardholders Report shall provide a listing of all cardholders who are exempt from following Destination Assurance procedures.

68) Device Status Events Report
The Device Status Events Report shall provide information on all status events for all devices in the SMS.

69) Dialup Events by Panel Report
The Dialup Events by Panel Report shall provide information on all dialup related events grouped by Intelligent System Controller.

70) Dialup Last Connect Time Report
The Dialup Last Connect Time Report shall provide a list of all online dialup panels and the last time that they were connected to the SMS database server.

71) Elevator Access Denials and Grants Report
The Elevator Access Denials and Grants Report shall provide information on all elevator related access denied and granted events including floor selected, time, card reader, badge, and cardholder name.

72) Elevator Dispatching Devices and Terminals Report
The Elevator Dispatching Devices and Terminals Report shall provide a listing of all elevator dispatching devices with the configured terminals.

73) Elevator Floor Assignments to Cardholders Report
76) The Elevator Floor Assignments to Cardholders Report shall list all cardholders that have access to a particular elevator floor list.

77) Emergency Events Report
The Emergency Events Report shall provide a listing of all emergency events over time.

78) Event Codes Report
The Event Codes Report shall provide information on all event code templates and event code mapping configurations.

79) Event Count by Panel Report
The Event Count by Panel Report shall provide a count of all events grouped by Intelligent System Controller. This report shall include a pie chart breakdown.

80) Fire Device Input or Output Report
The Fire Device Input or Output Report shall provide a listing of all fire inputs and outputs grouped by panel and fire device.

81) Global APB or MobileVerify Occupancy by Date Report
The Global APB or Mobile Verify Occupancy by Date Report shows the last known area accessed by each cardholder, sorted by date and time.

82) Global APB or MobileVerify Occupancy by Name Report
The Global APB or Mobile Verify Occupancy by Name Report shows the last known area accessed by each cardholder, sorted by cardholder.

83) Global I/O Linkages Report
The Global I/O Linkages Report shall provide a listing of all global I/O linkages, including the input events and output actions.

84) Guard Tour Configuration Report
The Guard Tour Configuration Report shall provide a listing of all configured guard tours, including checkpoints, actions, and messages.

85) Guard Tour History Report
The Guard Tour History Report shall provide a listing of all events associated with checkpoints that happened for each guard tour.

86) Hardware Panels Report
The Hardware Panels Report shall provide information on all top level hardware panels grouped by category including access panels, fire panels, intercom panels, personal safety panels and central station alarm receivers.

87) Holidays Report
The Holidays Report shall provide information on all system holiday definitions.

88) ILS Lock Authorizations by Cardholder Report
The ILS Lock Authorizations by Cardholder Report shall list ILS lock authorization levels assigned to cardholder/badge, sorted by cardholder.

89) ILS Lock Authorizations by Level Report
The ILS Lock Authorizations by Level Report shall list ILS lock authorization levels assigned to cardholder/badge, sorted by level.

90) ILS Lock Characteristics Report
The ILS Lock Characteristics Report shall list ILS lock configuration details.

91) ILS Lock Communications Report
The ILS Lock Communications Report shall list ILS lock wireless diagnostics.

92) ILS Lock Ownership Report
The ILS Lock Ownership Report shall list ILS locks owned by a cardholder.

93) Intercom Functions Report
The Intercom Functions Report shall provide information on all defined intercom functions.

94) Intercom Stations Report
The Intercom Stations Report shall provide information on all intercom stations, grouped by intercom exchange.

95) Intrusion Command Authority – Advanced Report
The Intrusion Command Authority – Advanced Report shall list all cardholders that have access level assignments configured to use advanced intrusion command authority.
96) Intrusion Command Authority – Global Report
The Intrusion Command Authority – Global Report shall list all cardholders who are assigned access levels with global intrusion command authority.

97) Intrusion Command Events Report
The Intrusion Command Events Report shall list all events associated with intrusion commands including device, cardholder name, and badge.

98) Intrusion Detection Areas Report
The Intrusion Detection Areas Report shall provide a listing of all intrusion areas grouped by panel.

99) Intrusion Detection Devices Report
The Intrusion Detection Devices Report shall provide a listing of all intrusion devices grouped by panel.

100) Intrusion Panel User Groups Report
The Intrusion Panel User Groups Report shall provide a listing of all intrusion user groups grouped by panel.

101) Last Location of Cardholders Report
The Last Location of Cardholders Report shall provide information on the last card reader accessed by each cardholder, sorted by cardholder name.

102) Locked Video Events Report
The Locked Video Events Report shall list all system events with associated locked video events.

103) Maps Report
The Maps Report shall provide a list of all available maps in the database.

104) Mobile Verify User Transaction Log Report
The Mobile Verify User Transaction Log Report shall provide a chronological log of all performed transactions.

105) Mobile Verify User Transaction Log by Operation Report
The Mobile Verify User Transaction Log by Operation Report shall provide a chronological log of all performed transactions grouped by operation.

106) Mobile Verify User Transaction Log by User ID Report
The Mobile Verify User Transaction Log by User ID Report shall provide a chronological log of all performed transactions grouped by User ID.

107) Module Details Report
The Module Details Report shall provide information about module definitions, grouped by parent panel.

108) Module Summary Report
The Module Summary Report shall list all modules, grouped by parent panel.

109) Monitor Stations Report
The Monitor Stations Report shall provide information on all monitoring stations defined in the SMS including which monitor zones and access panels are assigned to the monitoring station.

110) Monitor Zones Report
The Monitor Zones Report shall provide information on all monitor zone definitions.

111) NGP Panels Report
The NGP Panels Report shall provide information about NGP Panel definitions.

112) Overdue Visits Report
The Overdue Visits Report shall provide a listing of all scheduled visits that have not signed in.

113) Overstayed Visits Report
The Overstayed Visits Report shall provide a listing of all visitors logged into the facility, but whose badge or visit has expired.

114) Permission Profiles Report
119) The Permission Profiles Report shall provide information on permission profile definitions.
120) Personal Safety Transmitter Assignments Report
The Personal Safety Transmitter Assignments Report shall provide information on all personal safety transmitters and their assignments to cardholders and assets.
121) Personal Safety Transmitters Report
The Personal Safety Transmitters Report shall provide information on all personal safety transmitters.
122) Personnel in the Database Report
The Personnel in the Database Report shall provide information on all personnel in the database with basic information.
123) Personnel Without an Active Badge Report
The Personnel Without an Active Badge Report shall provide information on all personnel in the database that do not have an active badge assigned to them.
124) Personnel with Organizational Details Report
The Personnel with Organizational Details Report shall provide information on all personnel in the database with organizational details. This report is designed to work with the SMS standard cardholder layout.
125) Personnel with Personal Details Report
The Personnel with Personal Details Report shall provide information on all personnel in the database with personal details. This report is designed to work with the SMS standard cardholder layout.
126) Point of Sale Registers Report
The Point of Sale Registers Report shall provide a listing of all Point of Sale Registers configured in the SMS.
127) Precision Access Groups Report
The Precision Access Groups Report shall provide information on all precision access group definitions.
128) Reader Assignment to Cardholders Report
The Reader Assignment to Cardholders Report shall provide a listing of all card readers assigned to a cardholder, sorted by cardholder.
129) Reader Command Programming Configuration Report
130) The Reader Command Programming Configuration Report shall list all command programming readers along with the associated user and instant commands.
131) Reader Status Events Report
The Reader Status Events Report shall provide information on card reader status events, grouped by card reader.
132) Reader Timezone Schedules Report
The Reader Timezone Schedules Report shall provide information on all card reader timezone scheduling for card reader modes.
133) Readers Report
The Readers Report shall provide information on all card reader definitions grouped by access panel.
134) Receiver Account Alarm Activity Report
135) The Receiver Account Alarm Activity Report shall provide information on all alarm activity for receiver accounts including notes and elapsed times.
136) Receiver Account Areas Report
The Receivers Account Areas Report shall provide a listing of all receiver account areas, grouped by receiver account.
137) Receiver Account Groups Report
The Receivers Account Groups Report shall provide a listing of all receiver account groups and the receiver accounts contained in each group.
138) Receiver Account Zones Report
The Receivers Account Zones Report shall provide a listing of all receiver account zones, grouped by receiver account.

139) Receiver Accounts Report
The Receiver Accounts Report shall provide a listing of all receiver accounts in the SMS.

140) Receiver Accounts that Failed to Report Report
The Receiver Accounts that Failed to Report Report shall provide a listing of receiver accounts that failed to report during their duration.

141) Receiver and Receiver Account Events Report
The Receiver and Receiver Account Events Report shall provide a listing of all events that occurred on a receiver or receiver account.

142) Segment Badge Download Summary Report
The Segment Badge Download Summary Report shall provide information on each segment by listing the number of badges that must be downloaded to the access panels in that segment. This report shall only work on systems utilizing database segmentation.

143) Segments Report
The Segments Reports shall provide a listing of all segments defined in the SMS along with their options.

144) SNMP Agents Report
The SNMP Agents Report shall provide a listing of all SNMP Agents configured in the SMS.

145) SNMP Management Information Base Configuration
The SNMP Management Information Base Report shall list all MIB data grouped by enterprise.

146) System Servers Report
147) The System Servers Report shall provide a listing of servers defined on the system.

148) Text Instructions Report
The Text Instructions Report shall provide information on all text instructions defined in the SMS.

149) Timezones Report
The Timezones Report shall provide information on all timezone definitions.

150) User Permissions Report
The User Permissions Report shall provide information on all SMS users and their permissions.

151) User Transaction Log Report
The User Transaction Log Report shall provide a chronological log of all transactions performed on the SMS by users.

152) User Transaction Log by User ID Report
The User Transaction Log by User ID Report shall provide a chronological log of all transactions performed on the SMS by users grouped by User ID.

153) Users with Area Access Levels to Manage Report
The Users with Area Access Levels to Manage Report shall list all Area Access Manager users and the access levels that they manage.

154) Video Cameras Device Links Report
The Video Cameras Device Links Report shall provide information on all device links for each video camera.

155) Video Cameras Report
The Video Cameras Report shall provide information on all video cameras grouped by digital video recorder.

156) Video Events Report
The Video Events Report shall provide information on all SMS events with associated video events.

157) Video Servers Report
The Video Servers Report shall provide information on all digital video recorders.

158) Visits History Report
The Visits History Report shall provide information on all visits enrolled into the SMS.

159) Visitors Report
The Visitors Reports shall provide information on all visitors in the SMS.

160) Windows Event Log Errors Report
The Windows Event Log Errors Report shall provide information on all errors logged by the SMS to the Windows event log.

The report user interface in System Administration shall allow the System Administrator to filter on the UTC time columns.

The SMS shall provide filters for each report that, depending on the report that the System Administrator is running, will allow the System Administrator to filter any of the below listed criteria. The SMS shall allow reports to be filtered by any combination of card readers, date and time, cardholder first name and/or last name, area, Action Type, Details or Object, Alarm Acknowledgement and/or badge ID. The SMS will store all reports in the database so that all client workstations will have instant access to the report. The reports shall not be installed in a shared disk directory.

The SMS shall support advanced filters. The SMS shall allow reports to use the Time filter to span across multiple days to create shift reports. For example, a report shall be able to be run that shows all access grants that occurred Monday through Friday, but on during the hours of 8:00 AM to 5:00 PM on those days.

The SMS shall allow for cardholder related reports to be run from the Alarm Monitoring application of the SMS.

When running a report, the SMS shall alert the System Administrator if the report contains deprecated fields.

The current World Time Zone shall display on a report when it is run, along with report date or time.

The SMS shall allow System Administrators to specify card readers as either an ‘in reader’ or an ‘out reader’. The designation of these card readers will act as another filter to use in conjunction with the standard reports to produce ‘raw data’ which shall be exported to external systems such as Human Resources or Excel Spreadsheets which can crunch the data for Time and Attendance purposes.

The SMS reporting interface shall be available from the System Administration Module as well as the Alarm Monitoring application.

The SMS shall support configuring default printers for printing reports.

186. Ad-hoc Database Report Generator
The SMS must provide an ad-hoc customized report generator package integrated with the SMS’s database. This program shall allow the System Administrator to create reports using the relational database structure. Among other reports, a tabular type report shall be configurable which will detail any information from the database in a columnar format with headings, breaks, sub-totals and totals. The report must also be able to be created to produce a flat ASCII export file. Access rights shall be provided to allow the System Administrator the privilege of creating, deleting, updating, saving, processing, viewing and printing reports. The reports are to be printed on a dot matrix printer or on a laser printer. Report configuration shall use menu options and drop-down list boxes to define that database fields are to be used, linked, or joined. They shall also be used to specify conditions and column order, as well as describe the layout and headings.

187. Custom Report Writer
The SMS shall support an industry standard, off the shelf, custom report writer, such as Crystal Reports 11, or 11.5. The custom report writer shall support multiple report types including, but not limited to, multiple section reports, form style reports, conditional reports, query reports, and columnar reports. The custom report writer shall have BLOB Bitmap support and shall come standard with a formula editor with more than 160 built in functions for System Operators to manipulate data. It shall have export capabilities to ASCII files, Microsoft Mail, or ODBC file formats. The custom report writer shall be compatible with industry standard SQL databases, such as Microsoft SQL Server 2005 or Microsoft SQL Server 2008.

PCC Security Implementation
Pima Community College
NTD # 2009-0118-01

Security Management System
28 50 00 - 72
188. System Tape Backup
A mandatory requirement, the SMS shall provide tape backup and restore programs utilizing the multi-tasking capabilities of the SMS and operating system. These programs shall run concurrently with any other application. Database backup must occur dynamically while other alarm monitoring, badging, access control applications remain active.

The tape backup feature shall allow for three levels of tape backup; 1) Incremental, which will back up all changes to data and images that have changed since the last incremental tape backup, 2) System, which will back up the operating system and application files only, and 3) Full, which backs up all files.

A database snapshot shall occur prior to a tape backup and the actual backup shall be performed in the background, utilizing the benefits of the multi-tasking operating system, without interfering with the ability of System Operators to exercise other functions.

189. Client workstations
System Administrators shall have the ability to configure each client workstation on the SMS to utilize any combination of event printers, CCTV controllers, and video capture boards. For each printer or CCTV controller, System Administrators shall be able to select the port that the device is connected to on the client workstation and the communications speed.

190. PIN Numbers
The SMS shall have the ability to support up to nine (9) digit PIN Numbers for each cardholder in the SMS. PIN Numbers shall be created either manually through System Operator entry or generated randomly by the SMS. The SMS shall have the ability to be configured to allow for unique PINs for each cardholder and the ability to modify cardholder’s PIN numbers at a later date.

191. List Builder
System Administrators shall have the ability to pre-define information that will appear in each of the pre-defined drop-down lists. There shall be no limit to the number of items that shall be a part of a list. Lists can have items added to them or deleted from them at any time.

192. Archiving
The SMS shall allow System Administrators to archive offline history files to magnetic media. Offline files shall include access events and System Operator transactions that have been purged from the reportable database. The offline files MUST be in a “ready to import” format for easy insertion of information back into the online database. Different event types may remain in the database for different time periods according to the System Operator’s specification.

Any record older than the specified dates shall be purged to the offline history file for archiving. Reports shall be generated from the archived files if necessary. Archiving shall be a scheduled, automatic function.

193. Remote Dial-In Capabilities
The SMS shall support remote dial-in capabilities for SMS troubleshooting, SMS configuration, and alarm monitoring capabilities.

VAR and/or System Administrators shall be able to dial in to the CUSTOMER database server to troubleshoot the CUSTOMER’s system. This will allow System Administrators to locate any problem areas and, many times, fix the error over the telephone from a remote location.

Remote dial-in shall also be used for SMS configuration and/or alarm monitoring from remote locations using a client workstation. The client workstation shall have the ability to operate on a Laptop PC that meets the client workstation minimum specifications.

194. Reader Groups
a. The SMS shall support reader groups. The SMS’s Grouping form shall be used to:
   1) Specify the group or groups to which the reader belongs.
   2) Search for readers by group (The search for readers button is available from all of the forms in the Readers folder.)
3) Name and save lock group search criteria for future use.

b. Six (6) default reader group drop-downs are provided on the SMS’s Grouping form.

195. Mobile Enterprise Applications: This section is designed to be utilized in addition to, and in conjunction with, the rest of the SMS Functional Generic Specification. It is designed for use with those systems that deploy, or wish to deploy, the SMS Mobile Enterprise Architecture for Mobile Computing requirements.

The Mobile Enterprise Architecture is a mobile, synchronized database solution that is designed for customers with mobile computing needs. Mobile Enterprise functionality shall be a seamlessly integrated, robust solution that transports virtually all SMS client functions to a wearable, portable computer that connects to the network and SMS Server via 802.11b wireless Ethernet online, or as a standalone solution that can be synchronized with the SMS Server on an operational basis.

At a high level, Mobile Enterprise shall offer:
a. Wearable computers for mobile computing applications
b. Standard SMS software
c. Wireless network connectivity
d. Standalone operations
e. Central Database Storage Facilities
f. Data Synchronization Between Multiple Databases
g. Mobile Alarm Monitoring and System Administration Capabilities
h. Unlimited Expansion Capabilities
i. Open Architecture Design
j. Advanced Network Design
k. Integration with Digital Video, ID Credential Management, and Visitor Management Systems

196. The SMS shall support a multi-PC, multiple database synchronization architecture (herein after Mobile Enterprise Architecture) using a database server. The database server shall allow multiple wearable or mobile computers to be connected to it (via wired or wireless LAN or WAN architecture). In a stand-alone environment, connections shall occur only during synchronization.

197. The database server shall contain a master copy of all relevant system data. An unlimited number of mobile enterprise client workstations may be connected to the database server.

198. In a stand-alone environment the mobile enterprise computing PC shall contain a copy of all required core information obtained from the database server. This shall include, but not be limited to, cardholders, badges, badge types, and access permissions.

199. At predetermined, user-definable, periodic intervals, each of the stand-alone mobile enterprise computers shall connect to the database server to perform a database synchronization process.

200. In a wireless, online environment during daily SMS operation, each of the mobile enterprise client workstations shall connect locally to the database server via industry standard 802.11b wireless network connectivity. Mobile enterprise client workstations shall be any combination of system administration, alarm monitoring, digital video, visitor management, remote access level management, or ID management applications.

201. Unlimited system expansion and scalability shall be possible with the Mobile Enterprise architecture. There shall not be a limit to the number of mobile enterprise computing PCs that can be deployed.

a. Application Support

Mobile Enterprise shall support any SMS application on its mobile computing platform including:

1) Access Control
2) Alarm Monitoring
3) ID Credential Management
4) Digital Video
5) Intrusion Detection
6) Visitor Management

b. Platform Support
Mobile Enterprise shall be deployed onto a mobile PC computing platform. Minimum mobile computing platform specifications shall be as follows:
1) Operating System: Microsoft Windows 7 or 2008 or 2003 or XP or Vista
2) Processor: 600 MHz Transmeta Crusoe™
3) Size: 9.75 in. (L) x 3 in. (W) x 1.25 in. (D) (24.76 cm (L) x 7.62 cm (W) x 3.17 cm (D))
4) Weight: 22 oz (624 grams)
5) RAM: 128 MB DRAM
6) Hard Drive: 6 GB or greater
7) PC Card slots: Two Type II or one Type III
8) Temperature Range: 32 degrees F to 122 degrees F (0 degrees C to 50 degrees C)
9) Battery: Lithium Ion, Hot-Swappable
10) Run time: 7 to 12 hours on a two-battery system
11) Display: SVGA Indoor or Outdoor glass with Magnesium case

c. Mobile Verify
Mobile Enterprise shall support a Mobile Verify software option specifically designed for Mobile Enterprise Solutions, which shall provide the ability for an officer to use an optional scanner or card reader to automatically search the database for access privileges. The officer shall instantly be presented with the answer of either Access Granted or Access Denied based on the credential holder’s privileges. This functionality shall be accomplished in either standalone or online mode.
d. Network Connectivity
Mobile Enterprise shall be deployed using industry standard 802.11b wireless network technology. With its high throughput and long range, 802.11b shall operate in the unlicensed 2.4GHz frequency spectrum that is well established in corporate wireless markets.
e. Stand-alone Mode
Mobile Enterprise shall also be deployed as a stand-alone mode. In a stand-alone environment the mobile computing PC shall contain a copy of all required core information obtained from the database server in order to execute Mobile Verify functionality. This shall include, but not be limited to, cardholders, badges, badge types, and access permissions.
f. Login Privileges
Any mobile enterprise client workstation shall have the ability to log into the system for the purpose of System Administration, Alarm Monitoring, ID Credential Management, Mobile Verify, etc.
The System Administrator or System Operator at the mobile enterprise client workstation will have appropriate privileges based on their login ID and permissions for that particular user account as determined on the database server.
g. User Transactions
User transactions shall be logged on all mobile enterprise computing clients and shall be stored at the database server.

202. Badge Layout Creation Module: The SMS shall provide a Badge Layout Creation and Editing Module to allow for the creation of custom badge designs to be created by the CUSTOMER. The SMS shall support credit card, government, and custom credential sizes in either a landscape or portrait format.
a. Badge Layout Objects
The SMS shall support multiple object types, all of which shall be placed on the layout in any order and combination. These objects shall include alphanumeric text fields, database fields, photos, signatures, logos, graphics, shapes (square, circle, rectangle,
ellipse), and bar codes. Objects shall be placed onto the layouts through a Windows drag and drop process.

b. Advanced Database Field Driven Badge Layouts
The SMS shall support advanced functionality that allows cardholder database information to control what information is printed onto a cardholder’s credential. Thus, a single generic layout shall be created, and attributes such as colors, borders, logos, typefaces, backgrounds, etc. shall be determined by the information of a particular database field. For example, when ‘Marketing’ is entered in the Department field, a green background shall be printed on the badge. However, when ‘Engineering’ is entered in the Department field, a blue background shall be printed on the badge.

Any information displayed in a drop-down list shall have the ability to control any of the following credential attributes:
The SMS shall support insertion of extended ASCII codes into the Text property of objects within the badge layout.

c. Object Properties
System Administrators shall have the ability to edit each object placed onto the layout using a ‘Properties Form’ to customize each object on the layout.

1) Text and Database Objects
System Administrators shall be able to adjust the positioning of the object, its height and width, along with the object’s color and color fill style (solid, horizontal lines, etc.). Borders (if any), along with the border width and border style shall also be modifiable. The typeface of any text shall be user-definable (font, size, bold, italic, underline) as well as the alignment of the text inside of the object (left, center, right, top, middle, bottom). System Administrators shall be able to allow word wrapping of text within the object and shall be allowed to set the maximum number of characters allowed in the object.

2) Photo, Signature, and Graphic (logo) Objects
System Administrators shall be able to adjust the positioning of the object, its height and width, along with the object's color and color fill style (solid, horizontal lines, etc.). Borders (if any), along with the border width and border style shall also be modifiable. Attributes shall be available for auto sizing and scaling the photo, signature, or graphic that shall be located in the object. Keeping aspect ratio shall be an option. Alignment of the photo, signature, or graphic inside of the object (left, center, right, top, middle, and bottom) shall be available. System Administrators shall also be able to chromakey and/or ghost the photo or graphic. System Administrators shall also be able to tile the image or logo in any number of rows and columns across the background of the credential.

3) Shape Objects
System Administrators shall be able to adjust the positioning of the object, its height and width, along with the object's color and color fill style (solid, horizontal lines, etc.). Borders (if any), along with the border width and border style shall also be modifiable. System Administrators shall have the option of inserting square, circle, rectangle, or ellipse shapes.

4) Bar code Objects
System Administrators shall be able to adjust the positioning of the object, its height and width, along with the object's color and color fill style (solid, horizontal lines, etc.). Borders (if any), along with the border width and border style shall also be modifiable. System Administrators shall have the option of inserting square, circle, rectangle, or ellipse shapes.

The SMS shall allow System Administrators to encode any database field and/or other information onto the bar code, depending on the bar code type selected.

5) Object List
An object list shall be available to System Operators to allow them to select objects without clicking on them in the layout with the mouse. This shall be helpful when one object has been placed onto top of the other, making it difficult to select the object in the background with the mouse; or when System Operators wish to select an object without moving the object’s position on the layout.
6) Color Palette
The SMS shall support a Windows Color Palette capable of creating up to 16.7 million colors to be used in applying color to the various objects, shading, and/or borders in the badge layout.

7) Import of Badge Layouts
The SMS shall also allow for the importing of badges from a .bdg file.

8) Multiple Badge per Page Printing
The SMS shall allow for System Operators to print multiple badges to the same page. System Administrators can configure the SMS to print multiple badges to a pre-defined number of columns and rows to accomplish 2 up, 4 up, 6 up, or 8 up printing. This feature is useful when printing badges for visitors.

9) Working with Objects
A set of alignment tools shall be available to System Administrators to manage objects. ‘Move to Front’, ‘Send to Back’, ‘Move Forward’, and ‘Move Backward’ commands shall be available to allow objects to be placed on top of other objects.
The SMS shall support the rotation of objects in 90 degree increments (0 degrees, 90 degrees, 180 degrees, 270 degrees).
A zoom command shall be available to allow System Administrators to manage the layout in multiple views.
User-definable sample field data shall be available for ease of working with objects. When objects are placed onto a layout, the sample data will fill in to show the System Administrator what effect the object has on the layout.
System Administrators shall also be able to select the color of the PVC card that they are working with so they will see the effect that it has on the layout. They shall also be able to place the magnetic stripe outline on to the layout for ease of aligning other objects.
All Badge Layouts shall be placed in a gallery for previewing.

203. Screen Designer Tool
a. SMS Cardholder Standard Fields and Objects
The SMS shall support at a minimum the following standard fields for personnel information:
1) Last Name
2) First Name
3) Middle Initial
4) Social Security Number
5) Badge Type
6) Address 1
7) Address 2
8) City
9) State
10) Zip Code
11) Phone Number
12) Birth Date
13) Title
14) Department
15) Division
16) Location
17) Building
18) Floor
19) Office Phone Number
20) Extension
21) Signature
22) Last Reader Accessed
23) Record Last Changed
24) Badge ID
25) Issue Code
b. SMS Asset Standard Fields and Objects

SMS shall support at a minimum the following standard fields for asset information:

1) Scan ID
2) Asset Name
3) Acquired
4) Replace
5) Type
6) Subtype
7) Serial Number
8) Department
9) Assessed Value
10) Replacement Value
11) Last Inspection
12) Next Inspection
13) Record Last Changed
14) Photo
15) Photo Display
16) Last Reader Accessed
17) Assignment Button

c. SMS Visitor Standard Fields and Objects

SMS shall support at a minimum the following standard fields for visitor information:

1) Last Name
2) First Name
3) Middle Initial
4) Badge Type
5) Organization
6) Title
7) Address 1
8) Address 2
9) City
10) State
11) Zip Code
12) Office Phone
13) Extension
14) Last Changed
15) Last Reader Accessed
16) Record Last Changed
17) Badge ID
18) Issue Code
19) Number of Prints
20) Activation Date
21) Deactivation Date or Time
22) Badge Status
23) Photo
24) Photo Display
1) Host Name
2) Visitor Name
3) Status
4) Scheduled Time In
5) Scheduled Time Out
6) Actual Time In
7) Actual Time Out
8) Last Changed
9) Type
10) Purpose

e. User-definable Fields

Should the SMS standard fields not be suitable, System Administrators shall have the ability to modify any standard field to customize the cardholder, asset, and visitor forms as desired. The SMS shall also allow System Administrators to add custom fields in addition to or replacement of any standard fields on a minimum of thirty two (32) pages each of information for the cardholder, visitor, and visit forms and one page of information for asset. User-defined fields absolutely shall not be pre-defined, meaning only the labels can change while the properties cannot. System Administrators shall have a minimum of sixteen pages of which to design their screens with standard and custom fields.

f. System Administrators shall have the ability to modify the pages of information in any combination as follows:

1) Move standard database fields to different locations on the cardholder forms
2) Delete standard database fields that are not desired
3) Keep standard database fields in the same location as the factory ships them, but changing the label and/or any field attributes. For example, Zip Code may be changed to Postal Code and the attributes changed from a number field to text field for Canadian Installations
4) Add new fields to the cardholder forms each with their own unique set of attributes

g. Field Types

The SMS shall support, at a minimum, the following field types:

1) Text Fields
2) Date Fields
3) Numeric Fields
4) Drop-down Lists

h. Field Attributes

System Administrators shall be able to assign any combination of the following attributes to each field defined:

1) Positioning of the field on the form
2) From which page the field can be viewed
3) From which page the field can be edited
4) The font to be used for the information that will appear in the field. The SMS shall support all standard Windows fonts
5) The style to be used for information that will appear in the field. The SMS shall support bold, italic, both, and regular typeface styles
6) Any effects to be used for the information that will appear in the field. The SMS shall support strikeout and underline
7) Whether the field is required
8) Whether the field is to be indexed
9) Whether the field is unique
10) If a template is to appear in the field
11) If a default value will appear in the field

i. Field Styles

System Administrators shall be able to assign any combination of the following styles to each field defined:
1) Multi-line field
2) Horizontal Scroll
3) Vertical Scroll
4) Auto Horizontal Scroll
5) Auto Vertical Scroll
6) Enter means next line of text
7) Number
8) Uppercase
9) Lowercase
10) Read Only
11) Align Right
12) Password
13) Sunken
14) Border
15) Inside Edge
16) Raised
17) OEM Covert

j. Field Alignment and Width Tools
The SMS shall support the following field alignment tools to allow System Administrators to align fields and set uniform widths to fine tune the look and feel of the screens. The SMS shall allow System Administrators to select multiple objects simultaneously and align them to their desired position and/or set a uniform width. The following field alignment tools shall be able to be used in any combination:

1) Align all objects selected to the far left edge of the farthest left selected object
2) Align all right edges of selected objects to the right edge of the farthest right selected object
3) Align the tops of all selected objects to the top edge of the highest selected object
4) Align the bottom edges of all selected objects to the bottom edge of the lowest selected object
5) Align all selected objects to be vertically centered with respect to each other
6) Center all selected objects
7) Make all selected objects the same width as the smallest object selected
8) Make all selected objects the same width as the widest object selected
9) Make all selected objects the same height as the shortest object selected
10) Make all selected objects the same height as the tallest object selected
11) Evenly space all objects vertically between the two most outer objects
12) Evenly space all objects horizontally between the two most outer objects
13) Bring object to the front of the page
14) Send object to the back of the page

k. Tab Ordering
The SMS shall allow System Administrators to set the TAB order (the order in which the cursor moves throughout the fields) of the SMS when System Operators utilize the TAB key to move throughout the cardholder form.

204. Map Editor Module
The SMS shall support graphical map creation software that shall allow the import of map backgrounds from any standard ‘off-the-shelf’ drawing package in the formats listed below:

a. AutoCAD DXF (.dxf)
b. Bitmaps (.bmp, .dib)
c. JPEG (.jpg)
d. JIFF (.jif)
e. Zsoft PCX/DCX (.pcx, .dcx)
f. Adobe Photoshop (.psd)
g. CALS Raster (.cal)
h. GEM/Ventura IMG (.img)
i. IBM IOCA (.ica)
j. WordPerfect Raster (.wpg)
k. Macintosh PICT (.pct)
l. Portable Network Graphics (.png)
m. TIFF (.tif)
n. Windows Metafile (.wmf, .emf)
o. Targa (.tga)
p. Kodak Photo CD (.pcd)
q. Kodak Flashpix (.fpx)
r. Encapsulated Post Script (.eps)

These architectural type maps must allow the detailed layout of an entire structure, part of a structure, a floor or department within a building, or layout of the periphery of a facility. Once a map has been drawn, the System Administrator must have the ability to place system level icons of card readers, input and output points, video cameras, and other access control field hardware 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 must allow various maps to be associated with each area to provide for the creation of hierarchy of maps. Overview maps of an entire facility shall be able to be viewed as requested and nested maps shall be accessed from the overview map to enlarge a specific area or facility on the screen. Maps shall also support user-defined text that shall be placed onto the map background.

The SMS shall allow hardware device icons to be either static or part of a device group. Icons that are part of a device group shall allow the hardware device icon to change shape and/or color based on the current state of the device.

Maps shall have the ability to be printed and/or previewed from the Map Editing Module or the Alarm Monitoring application.

The SMS shall also support custom device icons to be used with the maps (.ico) files.

205. Import Module: The SMS shall support an import utility, which shall allow the CUSTOMER or VAR to import cardholder information into the SMS database. This shall allow the CUSTOMER or VAR to pre-populate the SMS database with existing cardholder data and/or add NEW records to an existing SMS database. The Import Module only supports SQL Server; it does not support Oracle. For Oracle,DataExchange must be used for data import.

The Import Utility shall be a 32-bit Windows application that shall be used to import standard ASCII delimited text files into the SMS. The import utility shall be utilized at the initial SMS setup and anytime a large number of records need to be imported into the SMS after the initial import. For example, a large university may import 10,000 records into the SMS during the initial SMS setup and then import 2,000 additional records each semester thereafter. The SMS shall check for duplicate records during the import, so that multiple copies of the same record are not added into the SMS database.

The import utility shall allow System Administrators to choose the delimiter for the ASCII file. This delimiter may be, but is not limited to, a comma, vertical bar, semi-colon, or asterisk. Fields in the SMS database, such as Address 2, that the CUSTOMER does not wish to use, may be left blank in the ASCII file.

The import utility shall be able to select the source drive where the ASCII delimited file is located as well as the destination drive where the SMS database is located.

The import utility shall also be able to import photos as part of the record into the SMS database. The SMS shall support the following file formats for the import of cardholder photos:
a. Bitmaps (.bmp, .dib)
b. JPEG (.jpg)
c. JIFF (.jif)
The SMS shall include a progress meter to show the System Administrator the percentage of the import complete when importing large quantities of records.

DataExchange: The SMS shall support an import or export utility that shall enable advanced System Administrators to import data and images into the SMS database and export data and images from the SMS database for use with third-party software systems.

The DataExchange Utility shall allow for bi-directional communications with external systems. It shall allow for the import into the SMS database and the export out of the SMS database personnel information, including images, through ASCII delimited files or XML files.

The import or export scripts shall run on schedule and shall be accomplished over the network. DataExchange is ideal for customers who wish to have a base line level of integration with third-party external systems such as those used for Time and Attendance and Debit Card systems. Database import and export scripts shall be stored in the SMS database. A user interface shall allow for the generation of import and export scripts. When configuring or running a DataExchange script, the SMS shall alert the System Administrator if deprecated fields are being used.

The file used for import or created by export shall have the ability to be structured in a wide variety of ways, but shall always be in either ASCII text, Unicode text, XML, or Database format. System Administrators can configure the import procedures to put the new data into any of the tables of the SMS database. As such, export data shall be taken from any tables in the SMS database.

a. File Imports

DataExchange shall allow data to be imported into the SMS database. Importing of information shall occur in one or more of the following methods:

1) Add - The data in the file shall be added to the database. If a particular record is already in the database, an error shall occur and the record shall be rejected and placed in an error log.

2) Change - If a record in the file exists in the database, the record shall be modified according to the layout configuration specified. Records in the file that don’t already exist in the database shall be rejected and placed in an error log file.

3) Delete - If a record in the file exists in the database, it shall be deleted.

4) Add or Modify - If a record in the file exists in the database, it shall be replaced according to the layout configuration you specified. Records that don’t already exist shall be added to the database.

b. DataExchange shall support a minimum of the following image file formats to be imported into the SMS database:

1) Adobe Photoshop 3.0 (PSD)
2) CALS Raster (CAL)
3) Delrina WinFax Group 3 (FAX)
4) Delrina WinFax Group 4 (FAX)
5) Encapsulated PostScript (EPS)
6) FAX Group 3 (FAX)
7) FAX Group 4 (FAX)
8) GEM Image (IMG)
9) IOCA or IBM Image Object Content Architecture (ICA)
10) JIFF or JPEG File Interchange Format (JPG or JIF)
11) JPEG Tagged Interchange Format (JTIF)
12) Kodak FlashPix (FPX)
13) Kodak PhotoCD (PCD)
14) LEAD CMP (CMP)
15) Macintosh Pict Format (PCT)
16) MacPaint (MAC)
17) OS/2 Bitmap (BMP)
18) Portable Network Graphics (PNG)
19) SUN Raster Format (RAS)
20) Truevision TARGA (TGA)
21) Microsoft Paint (MSP)
22) Windows Bitmap (BMP)
23) WordPerfect Format (WPG)
24) Zsoft PCX/Multipage PCX (PCX/DCX)

DataExchange shall utilize an error log that shall report all errors that occur during a file import. Any and all errors can then be viewed from this log, corrected, and the import shall run a second time to download the corrected records.

DataExchange must allow imported changes to be downloaded to Intelligent System Controllers on a near real-time basis as information is being imported into the database.

c. Exporting Data
DataExchange shall allow data to be exported from the SMS database. Any combination of SMS database fields shall have the ability to be exported to a Database or Unicode text file.

d. Data Expressions
DataExchange shall support run-time data generation to support customer business logic. Following expression types shall be provided:

1) Constants
This type of expression shall provide import or export with data that doesn't change like “5” or “Employee”. The System Administrator shall configure the value. Constant expressions shall be able to be parts of other expressions.

2) Increments
Similar to numerical constants, but changes as import or export progresses. For example: “1” for the first record, “3” for the second, “5” for the third etc. The System Administrator shall configure a base value (“1” in example) and increment (“2” in example).

3) Lookups
Lookup expressions query the SMS database with System Administrator provided data and return query result. For example, System Administrator data contains a department name such as “Engineering”, but to import a record department ID is needed. The System Administrator shall configure a lookup on DEPT table with NAME as a source field and ID as a return field. So lookup with “Engineering” will return “2”. Lookup expressions shall be cascaded or be parts of other expressions (such as conditional expressions).

4) Conditional expressions
Conditional expressions evaluate a comparison between two pieces of data to either a true or false result, and based on that result return one or the other configured user data.
Conditional expressions can be cascaded or be parts of other expressions (such as lookup expressions).

An example of an expression returning file data would be something like the imported data wants to use the default badge type business rule for the deactivate date when adding a new badge. However, if a badge already exists for the cardholder, use it's deactivate date.

e. Import or Export Filters
TheDataExchange shall allow System Administrators to select a subset of data for export or database import operations. SQL filter shall be used do define which records would be selected for the import or export.

207. SMS Server Redundancy

a. The SMS shall support multiple levels of fault tolerance and SMS redundancy listed and described below:
1) Hot Standby Servers
2) Clustering
3) Disk Mirroring
4) RAID Level 10
5) Distributed Intelligence

b. Hot Standby Server Solution
The SMS shall support a fault tolerant server and redundant database architecture. It shall allow for normal operations to occur in the event that the Database Server fails. In the event of a server failure, the switch over to a backup server shall be automatic. System Operator intervention for switch over shall not be acceptable.
The SMS shall utilize two servers, which shall be configured identically. One server shall be designated as the Primary Server and the other shall be designated as the Backup Server. The Primary Server shall be the main server that is in use when the SMS is operating under normal conditions.
The SMS shall mirror the database information from the Primary Server to the Backup Server. This mirroring shall be conducted through standard local area network (LAN) communications. There shall absolutely not be any proprietary communication links between the Primary and Backup Servers.
All access control field hardware shall be configured for both the Primary Server and the Backup Server. Both the Primary and Backup Servers shall recognize the same TCP/IP ISC address on the network.
If the Backup Server is not running or receiving the mirrored files from the Primary Server, the Primary Server shall save the changes locally. Upon restored communications to the Backup Server, this information shall be automatically sent to the Backup Server.
In the event that the Primary Server fails, the Backup Server shall sense that the Primary Server has failed and is no longer on the network. The Backup Server shall check to see if the Primary Server is online every five seconds.
Upon sensing Primary Server failure, the Backup Server shall automatically initiate itself as the Primary Server and shall begin communication with the Intelligent Fields Panels. ABSOLUTELY NO SMS OPERATOR INTERVENTION SHALL BE REQUIRED. A message shall be broadcast to all client workstations on the network that the Primary Server has failed and the Backup Server has taken control. This process shall take no longer than two minutes to accomplish.
Once the Primary Server comes back online with the SMS, the Primary Server and Backup Server shall be able to be re-synchronized though automatic operation and resume normal operations. The synchronization process shall be fast, efficient, and take no more than five minutes.
c. Clustering
The SMS shall support a fault tolerant cluster server architecture. It shall allow for normal operations to occur in the event that the Database Server fails. In the event of a server
failure, the switch over to a backup server shall be automatic. System Operator intervention for switch over shall not be acceptable.

The SMS shall utilize two servers, which shall be configured identically. One server shall be designated as the Primary Server and the other shall be designated as the Backup Server. The Primary Server shall be the main server that is in use when the SMS is operating under normal conditions.

The SMS shall use shared-media technology. This shall incorporate a third piece of hardware (for example: Dell PowerVault), which shall house the hard disk to be referenced by both servers. Since accessible media is dependent upon a third piece of hardware, emphasis shall only be placed upon the health status of the shared-media device. If the status of the shared-media device remains healthy, server up time is of no consequence to data integrity.

The shared-media device provides only a single point of failure. If this device fails, then data cannot be accessed. A dual point of failure shall be achieved by incorporating two shared-media devices that are mirrored (for example: two stacked mirrored Dell PowerVaults).

All access control field hardware shall be configured for both the Primary Server and the Backup Server. Both the Primary and Backup Servers shall recognize the same TCP/IP ISC address on the network.

In the event that the Primary Server fails, the Backup Server shall sense that the Primary Server has failed and is no longer on the network. The Backup Server shall check to see if the Primary Server is online every 5 seconds.

Upon sensing Primary Server failure, the Backup Server shall automatically initiate itself as the Primary Server and shall begin communication with the Intelligent Fields Panels. ABSOLUTELY NO SMS OPERATOR INTERVENTION SHALL BE REQUIRED. A message shall be broadcast to all client workstations on the network that the Primary Server has failed and the Backup Server has taken control. This process shall take no longer than 2 minutes to accomplish.

Once the Primary Server comes back online with the SMS, the Primary Server shall resume normal operations.

d. Disk Mirroring

The SMS database server shall protect data against failure of a hard disk or hard disk controller by providing a disk mirroring configuration. The disk mirroring configuration shall allow data to be stored on dual hard disks running simultaneously. When any client workstation or Intelligent System Controller sends data to the database server, it shall be stored to both sets of hard disk drives. In the event any component on one channel fails, the other disk drive continues to operate without data loss or interruption. The SMS shall also send a warning message indicating that one disk drive has failed.

e. RAID Level 10

The SMS shall offer a Fault Tolerant Redundant Array of Independent Disks Level 10 (RAID Level 10) with a hot standby disk. RAID Level 10 shall provide redundancy of disk storage, controller channels and power supplies. Each array must contain a disk drive, high efficiency power supply, and cooling fan. This technology shall use multiple drives to store data with distributed parity, thereby ensuring data protection in an environment in which data is safe and easily restorable in the event of a hard disk failure. In the event a single drive within the array fails, a "Hot Standby Hard Disk" shall be available online and automatically switched with the failed unit.

The network administrator shall be able to replace the failed drive without taking the database server down, and it shall then become the hot standby. The array software shall rebuild the lost data from parity information stored on the other drives in the array. This entire procedure shall have no effect on the operation of the SMS and shall be automated.

f. Distributed Intelligence

In the event SMS communications is lost or the database server fails, Intelligent System Controllers shall provide complete control, operation and supervision of all monitoring.
and control points. The ISC shall be configured with a UPS battery, which shall support the ISC for a 24 hour duration. The ISC shall be installed with enough memory to support up to 10,000 cardholders/100,000 events in a minimum configuration and be expandable to up to 250,000 cardholders/1,000,000,000 events.

The SMS shall incorporate performance tests and precautions so as to avoid SMS failure. In the event of a failure, transactions are to be stored in an ISC First In First Out (FIFO) buffer until the ISC comes back online, at which time all data is uploaded to the database server. The ISC shall register as online with the database server when communications are re-established. Should the ISC buffer fill and events are overwritten, an event will appear in the Main Alarm Monitoring Window notifying the System Operator that events were overwritten. The ISC shall send a time/date stamp of the last record or table update in its memory and request any new data changes or cardholder records which have changed since that time or date stamp. A complete download of database and access tables shall not be required because of offline operation.

208. DataConduIT: The SMS shall allow, through standard API toolkits, System Administrators to expose specific SMS data and events that are relevant to IT information or other third-party systems. Conversely, the SMS shall allow, through these same API toolkits, System Administrators to accept and process information exposed from the IT information or other third-party systems. This shall permit System Administrators to develop scripts and applications that allow events in either the IT domain to cause appropriate actions in the Security domain, and vice versa.

Using the toolkit, the following shall be a sample of the integration opportunities available:

a. When a cardholder account is created in the SMS, DataConduIT shall create a Windows 7 or 2008 or 2003 or XP Active Directory Account for that person. The Windows account name shall be derived from the SMS cardholder name. The SMS account and the Windows account shall then be linked to the same person.

b. When a user’s Windows 7 or 2008 or 2003 or XP Active Directory Account is created, DataConduIT shall create a SMS cardholder account, badge, and access rights. The SMS account and the Windows account shall then be linked to the same person. A cardholder’s phone number changes in the SMS. The new phone number shall be propagated through DataConduIT to the associated user account in the company’s Active Directory.

c. When a cardholder’s access badge is disabled, DataConduIT shall automatically disable that cardholder’s other IT user accounts.

d. Conversely when a user’s Windows or other Active Directory or LDAP account is disabled, DataConduIT shall deactivate the cardholder’s access badge in the SMS.

e. A user’s Windows account for PCs in a research lab is normally deactivated. When a cardholder cards into the research lab, DataConduIT shall activate the user’s Windows account for the computers in the research lab.

f. A third-party system acknowledgment of pending alarms in the SMS database.

All business rules pertaining to cardholders, badges, access levels, and linked accounts shall be enforced when a cardholder, badge, access level, or linked account is added, modified, or deleted. Clients shall not be able to make any writes that would be invalid if made through the SMS’s System Administration module.

g. SMS API Toolkit Operations

1) Operations

DataConduIT clients shall be able to add new cardholders and modify or delete existing cardholders, visitors, visits, biometrics, and images.

DataConduIT clients shall be able to add new badges and modify or delete existing badges.

DataConduIT clients shall be able to add and delete linked accounts. Modification of existing linked accounts shall not be permitted.

DataConduIT clients shall be able to view directory definitions. Modification of existing directories shall not be permitted.

2) Software Events
DataConduIT clients shall be able to register to receive notification when any of the following software events takes place:
   a) A person is added, modified, or deleted (including the person primary segment assignment)
   b) A badge is added or deleted, or its badge status changes
   c) A linked account is added or deleted

3) Hardware Events
DataConduIT clients shall be able to register to receive notification when any access control field hardware events take place.
This shall include access to areas, elevator readers, and assets, and for access attempts under duress.
This shall include the acknowledgment of pending alarms in the SMS database.

h. Accepting Custom Incoming Alarms and Events
The SMS shall accept generic or custom incoming events from third-party systems to be displayed in the Main Alarm Monitoring Window, similar to other SMS alarms. In addition, it shall be possible to configure where to route these alarms.
The SMS shall allow the Main Alarm Monitoring Window to represent the following:
   1) Source – a text representation of the object or device that generated the event
   2) Date or Time – the date and time when the event occurred
   3) Description – text of up to 80 characters that describes the event
   4) Additional Text – additional text of up to 1,000 characters associated with the event

i. DataConduIT Devices and Sub-Devices
The SMS shall be able to support downstream devices and sub-devices through DataConduIT. The configuration for these devices shall occur in the DataConduIT Source folder in System Administration.

j. Event Generation with Devices and Sub-Devices
The SMS shall be able to generate Access Granted and Access Denied events from a DataConduIT source, Device, or Sub-Device. The SMS shall also be able to pass the badge identification number along with the access granted or denied. This shall report to the DataConduIT source.

209. Open Protocol Interface
a. The SMS shall provide a set of standard Application Programming Interfaces (API’s) and supporting documentation that allows hardware manufacturers and software application developers to interface their products into the SMS. The Application Programming Interfaces shall allow requests to occur from CUSTOMER to interface a third-party hardware or software solution based on SMS open architecture and SMS device independence.
b. There shall be two components to the Application Programming Interfaces. There shall be a device interface and an application interface.
c. The device interface shall allow extensibility to the number and types of hardware devices supported by the SMS. Each individual piece of hardware shall have its own “driver” that shall understand how to communicate with the SMS hardware. These “drivers” or "device translators" shall translate a set of generic commands into specific device commands.
d. The device translators shall be implemented as COM (Component Object Model) objects so that they shall be loaded and unloaded as needed. Each device translator shall support certain interfaces that support a specific set of commands or methods. Some examples of typical interfaces could include an Access Control Interface for access control hardware, a Video Interface for DVR and NVR hardware, an Intercom Interface for intercom systems, an Intrusion Interface to support alarm inputs, etc. A particular device translator shall support many interfaces.
e. The main application that shall be used to control the various device translators is the SMS Communication Server (SCS). The SCS shall be the application that manages and sends the commands to the device translators. Other modules including Alarm Monitoring or System Administration shall communicate with the hardware devices by sending commands to the SMS Communication Server, which shall then send the commands on to the correct device or devices.

f. The device interface shall allow the software interface of any hardware device to be controlled and monitored via the SMS Alarm Monitoring application. This shall preserve customer investments in existing equipment as well as allow for system expansion to occur through the interface of the latest hardware technologies.

g. The application interface shall allow information to be exchanged between the SMS and other applications. The application interface shall provide the functions for interacting with the SMS. This includes the ability to extract information from the SMS database as well the ability to download, control and monitor information for all field hardware including access control panels, digital video systems, fire panels, alarm panels, intercom system, etc.

h. All functions of the application interface shall be defined in such a way that any Windows application or development environment with the ability to make “C” calls should be capable of making use of the API.

210. Open Supervised Reader Interface

a. The SMS shall provide connectivity to proximity and smartcard readers which provide continuous supervision and monitoring of reader processor and wiring integrity by means of a non-proprietary communications protocol standard. Supervision methods that simply supervise wiring or measure current draw are not acceptable, since they do not insure that the reader’s microprocessor is actually operational. Likewise, proprietary protocols which are sole sourced or licensed for a fee are not acceptable, since they limit potential future expansion options for the SMS.

b. The preferred protocol is the Open Supervised Device Protocol (OSDP), since it is non-proprietary and meets the requirements stated above. Alternative supervised reader interface protocols will be considered only if they meet all of the technical requirements of this section AND can be shown to be non-proprietary.

1.17 Network Account Management

The SMS shall support a Network Account Management module. The SMS’s Network Account Management Module shall integrate SMS cardholders with external user network accounts. Through linked accounts, System Administrators shall be able to perform a set of administrative tasks in Windows domains from the System Administration Module. The Network Account Management functionality shall also enable System Administrators to create a link between physical access control and logical domains. The SMS shall additionally be combined with the management of cardholders’ digital certificates stored on a smart card.

a. The integration shall provide a number of benefits, including the ability to do the following:

1) Perform administrative functions on Windows user accounts from within the SMS Administration Module.

2) Enable interaction between Physical Access Control Cardholders and Windows logical domains. For example, if badge is lost, a designated Windows account shall disable.

3) Control access to Computer Anti-Passback Areas

4) Issue Windows 2008 or 2003 Smart Card Logon and Smart Card User certificates on the user's smart card.

5) Add a New Account
During creation of cardholder records, System Operators shall select an option to create a network account for a new cardholder. The selected network account type shall determine the Windows 2008 or 2003 domain and a set of permissions for the new account.

6) Lost Badge
If a cardholder loses their badge, the System Operator shall change the reported badge status from Active to Lost. When the badge status is changed, all of the cardholder's linked network accounts automatically shall be disabled.

7) Computer Anti-Passback Area Access
Customer has set a security policy, which only allows access to computers in designated areas to personnel physically present in these areas. An employee must present a badge to the card reader in order to enter and exit these secure areas. A cardholder has access levels that allow him to enter secure area A. In addition, he has a network account of type B, which allows him access to computers in area A. When the cardholder gets "access granted" on entry reader of area A, his computer account of type B is enabled. When the cardholder leaves the area his network account becomes disabled.

k. System Operator Activity Logging
The SMS shall provide full System Operator activity tracking of critical keyboard functions. The activity log shall be comprehensive, recording the date and time of the activity, the client workstation at which the activity was performed, the System Operator who performed the activity, the program the activity occurred in, and the function that was performed within it. The SMS shall record any and all changes to the database made by all System Operators.

The SMS shall log all System Operator functions, including System Operator login and System Operator logout; Additions, Changes, and Deletions to Cardholder Management; New Badge, Print Badge, and Update Badge; and other critical database functions. The SMS shall log changes made to the access control configurations: Changes of access levels, holidays, timezone changes, card readers, and other critical items. The SMS shall log changes made to the digital video configurations including changes to digital video recorders, cameras, device links, and other critical functions. The SMS shall log changes made to the asset management configurations including changes to asset readers, assets, asset assignments and other critical functions. The SMS shall log changes to the visitor management configurations including the enrollment of visitors, assignment of visitors to cardholders, scheduling visits, and other critical functions.

The SMS shall log changes to the intrusion detection management configurations including the configuration of areas and zones, arming or disarming areas, and other critical functions. The SMS shall log activity of System Operators performing SMS alarm monitoring; that is, alarms acknowledged, cleared, output control activity, trace, and other functions. The SMS shall permit the System Administrator to define the number of day's worth of activity to keep online before the System Administrator purges the oldest data offline. The activity log will have a field to show the number of total System Operator events that are currently stored in the database. The number of events to keep online shall only be limited by the amount of disk space available on the database server. The SMS shall provide a System Operator activity report to query the above information available in the SMS database. Client workstation, System Operator, date and time, or other selection criteria shall sort the report. On those occasions when historical data shall be needed, the System Operator activity report shall be generated from an archived database as well as from the active SMS database.

l. Alarm or Event Activity Logging
The SMS shall provide full access or alarm or event activity logging. The activity log shall provide comprehensive logging of date and time of the transaction, where the transaction occurred, acknowledgment information, and any System Operator actions.
The SMS shall log all access grants, access denies, alarm actives, asset denies, and other critical and non-critical alarms. The SMS shall give System Administrators the ability to choose when to log certain types of alarms.

The log shall be broken down into the following categories: Events and Alarm Acknowledgements, User Transactions, and Visits. For each type of alarm, the System Administrator can set how long to keep each group of events. For example, visits may only be kept in the history file for 7 days while User Transactions may be kept for one year.

The activity log will have a field to show the number of total events that are currently stored in the database. The number of events to keep online shall only be limited by the amount of disk space available on the database server.

The SMS shall log a minimum of 1,000,000 events before the System Administrator purges the oldest data to an offline file. The hard drive space required to store 1,000,000 events shall not exceed 40 MB.

The SMS shall provide activity reports to query the above information available in the SMS database. The reports shall be sorted by client workstation, alarm type, date and time, or other selection criteria. On those occasions when historical data shall be needed, the activity reports shall be generated from an archived database as well as from the active SMS database.

m. Encryption of PIN Codes inside the Database Server

The SMS shall encrypt all cardholder PIN codes such that no one, including the System’s Administrator, shall have access to cardholder PIN codes through the application or through the database server.

n. Access Control Reports

There shall be a minimum of 140 standard SMS reports provided with the SMS. All reports MUST be stored in the SMS database and MUST be able to be viewed from any SMS client workstation with proper permissions. Reports shall use UTC time. The SMS shall allow the SMS USER to e-mail reports based on system events or on a user-defined schedule. The standard reports that shall be included with the SMS are described below:

1) Access Denials and Grants by Reader Report

The Access Denials and Grants by Reader Report shall provide information on all access denials and granted events including time, card reader, badge, and cardholder name, sorted by card reader.

2) Access Denials, Grants, and Other Badge Events Report

The Access Denials, Grants, and Other Badge Events report shall provide information on all badge related events including time, reader, badge, and cardholder name.

3) Access Denied Event Report

The Access Denied Event Report shall provide information on all access denied events including time, card reader, badge, and cardholder name. It shall also include the following events: Interlock Area Busy, Cannot Open Door: Interlock Area Busy, Exit Request Denied: Interlock Area Busy, and DURESS - Interlock Area Busy.

4) Access Denied Events, by Reader

The Access Denied Events, by Reader Report shall provide information on all access denied events including time, card reader, badge, and cardholder name, sorted by card reader. It shall also include the following events: Interlock Area Busy, Cannot Open Door: Interlock Area Busy, Exit Request Denied: Interlock Area Busy, and DURESS - Interlock Area Busy.

5) Access Granted Events Report

The Access Granted Events Report shall provide information on all access granted events including time, card reader, badge, and cardholder name.

6) Access Granted Events by Reader Report

The Access Granted Events by Reader Report shall provide information on all access granted events including time, card reader, badge, and cardholder name, sorted by card reader.

7) Access Groups Report
The Access Groups Report shall provide information on all access groups and the access levels contained in each group.

8) Access Groups with Levels Report
The Access Groups with Levels Report shall provide information on all access group definitions including access level details.

9) Access Level Assignments to Cardholders Report
The Access Level Assignments to Cardholders Report shall list each access level with a listing of each cardholder that has that access level assigned to them.

10) Access Levels Assignment to Cardholders, By Segment Report
The Access Levels Assignment to Cardholders, By Segment Report shall provide information on all cardholders with access levels, sorted by segment. Only personnel with assigned access levels shall be included in the report. This report shall also summarize the total number of badges that will need to be downloaded to each segment. This report only shall only work on a system utilizing database segmentation.

11) Access Levels Report
The Access Levels Report shall provide information on all access level definitions.

12) Access Panels Report
The Access Panels Report shall provide information on all access panel definitions.

13) Active Visits by Cardholder Name Report
The Active Visits by Cardholder Name Report shall provide information on all visits that are currently active (not signed out) grouped by cardholder name.

14) Active Visits by Host Name Report
15) The Active Visits by Host Name Report shall provide information on all visits that are currently active (not signed out) grouped by Host Name.

16) Active Visits by Visitor Name Report
The Active Visits by Visitor Name Report shall provide information on all visits that are currently active (not signed out) grouped by Visitor Name.

17) Alarm Acknowledgments Report
The Alarm Acknowledgments Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes.

18) Alarm Acknowledgements by Definition Report
The Alarm Acknowledgements by Definition Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by Definition.

19) Alarm Acknowledgments by System Operator Report
The Alarm Acknowledgments by System Operator Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by System Operator.

20) Alarm Acknowledgements by Panel Report
The Alarm Acknowledgements by Panel Report shall provide information on all alarm acknowledgments including the alarm information and acknowledgment notes, sorted by Intelligent System Controller Panel.

21) Alarm Configuration Report
The Alarm Configuration Report shall provide alarm configuration summary information.

22) Alarm Input Events Report
The Alarm Input Events Report shall provide information on all alarm input events sorted by date.

23) Alarm Panel Inputs Report
The Alarm Panel Inputs Report shall provide information on all alarm panel inputs grouped by access panel and alarm panel.

24) Alarm Panel Local Linkage Report
The Alarm Panel Local Linkage Report shall provide information of all input and output linkages within an ICM.

25) Alarm Panel Outputs Report
The Alarm Panel Outputs Report shall provide information on all alarm panel outputs grouped by access panel and alarm panel.

26) Alarm Panels Report

The Alarm Panels Report shall provide information on all alarm panel definitions grouped by access panel.

27) All Cardholders with Logical Access Report

28) The All Cardholders with Logical Access Report shall list all cardholders that have linked accounts through logical access.

29) All Events Over Time Report

The All Events Over Time Report shall provide a listing of all event types over time.

30) All Events Over Time with Local Panel Time Report

31) The All Events Over Time with Local Panel Time Report shall provide a listing of all event types over time. This report also shows the time an event occurred in the panel's time.

32) All Events Over Time with Unique Alarm ID Report

The All Events Over Time with Unique Alarm ID Report shall provide a listing of all event types with an unique alarm ID over time.

33) Anti-Passback Events Report

The Anti-Passback Events Report shall provide a listing of all anti-passback events over time.

34) Area Anti-Passback Configuration Report

The Area Anti-Passback Configuration Report shall provide a listing of all anti-passback areas, including the reader entrances and exits.

35) Area Configuration Report

36) The Area Configuration Report shall list all areas, including the reader entrances and exits.

37) Area Entrance History Report

The Area Entrance History Report shall provide a history of all cardholders enter anti-passback areas, sorted by area and date.

38) Asset Classes Report

The Asset Classes Report shall provide information on all asset classes and the asset groups to which they belong.

39) Asset Events Report

The Asset Events Reports shall provide information on all asset events.

40) Asset Groups Report

The Asset Groups Report shall provide information on all asset groups and the classes they contain.

41) Asset Types Report

The Asset Types Report shall provide information on all asset types defined with all associated subtypes.

42) Assets by Scan ID Report

The Assets by Scan ID Report shall provide information on all assets grouped by Scan ID.

43) Assets by Type Report

The Assets by Type Report shall provide information on all assets grouped by asset type and subtype.

44) Assigned Assets by Cardholder Report

The Assigned Assets by Cardholder Report shall provide information on all currently assigned assets grouped by cardholder.

45) Assigned Assets by Scan ID Report

The Assigned Assets by Scan ID Report shall provide information on all currently assigned assets grouped by Scan ID.

46) Assigned Assets by Type, Scan ID Report

The Assigned Assets by Type, Scan ID Report shall provide information on all currently assigned assets grouped by type and Scan ID.
47) Audio Notifications and Instructions Report
The Audio Notifications and Instructions Report shall list all audio notifications and instructions in the database.

48) Badge Type Configuration
The Badge Type Report shall provide a listing of all Badge Types.

49) Badges by Deactivation Date Report
The Badges by Deactivation Date Report shall list all badges by deactivation date. Shall be used to determine which badges are about to deactivate.

50) Badges Without Access Levels Report
The Badges Without Access Levels Report shall provide information on all Badges that do not have any access levels assigned to them. Badges with access levels assigned to them shall not be listed in this report.

51) Card Formats Report
The Card Formats Reports shall provide information on definitions of all Magnetic and Wiegand card formats in the SMS.

52) Cardholders Access to Readers Report
The Cardholders Access to Readers Report shall provide a listing of each card reader along with which cardholders have access to that card reader. Includes associated access level and timezone.

53) Cardholder Exit or Entry Report
The Cardholder Exit or Entry Report shall provide information on all user-defined Exit or Entry information on a per cardholder basis. It shall list the time a cardholder swipes their badge at a designated ‘In’ reader and the time they swiped their badge at the corresponding designated ‘Exit’ reader.

54) Cardholder Photo Gallery Report
The Cardholder Photo Gallery Report shall provide cardholder names and photos, sorted by last name.

55) Cardholder Time and Attendance Report
The Cardholder Time and Attendance Report shall pair each in-time with an out-time for cardholders gaining entry to time and attendance readers.

56) Cardholders by Badge Type Report
The Cardholders by Badge Type Report shall provide information on all cardholders sorted by badge type. No access levels are shown in this report and cardholders that have not been assigned a badge type will not be reported.

57) Cardholders by Last Name Report
The Cardholders by Last Name Report shall provide information on all cardholders sorted by last name, with badges but not access levels. Only personnel with badges assigned shall be included in this report.

58) Cardholders Located in Each APB Area by Date Report
The Cardholders Located in Each APB Area by Date Report shall provide a list of all cardholders located in each anti-passback area, sorted by area and date.

59) Cardholders Located in Each APB Area by Name Report
The Cardholders Located in Each APB Area by Name Report shall provide a list of all cardholders located in each anti-passback area, sorted by area and cardholder name.

60) Cardholders with Access, by Badge Type Report
The Cardholders with Access, by Badge Type Report shall provide information on all cardholders with access and precision access levels, sorted by badge type. Only personnel with active badges and access levels shall be included in this report.

61) Cardholders with Access by Last Name Report
The Cardholders with Access by Last Name Report shall provide information on all cardholders with access and precision access levels, sorted by last name. Only personnel with active badges and access levels shall be included in this report.

62) CCTV Instructions Report
The CCTV Instructions Report shall provide summary information on all CCTV instructions in the database.

65) Continuous Video Report
The Continuous Video Report shall provide a listing of all of the times continuous video is archived.

66) Current Visits Report
The Current Visits Report shall provide a list of all currently signed in visits.

67) Destination Assurance Configuration Report
The Destination Assurance Configuration Report shall provide a listing of all card readers configured for Destination Assurance with their associated lead times to proceed to the next defined card reader.

68) Destination Assurance Exempt Cardholders Report
The Destination Assurance Exempt Cardholders Report shall provide a listing of all cardholders who are exempt from following Destination Assurance procedures.

69) Device Status Events Report
The Device Status Events Report shall provide information on all status events for all devices in the SMS.

70) Dialup Events by Panel Report
The Dialup Events by Panel Report shall provide information on all dialup related events grouped by Intelligent System Controller.

71) Dialup Last Connect Time Report
The Dialup Last Connect Time Report shall provide a list of all online dialup panels and the last time that they were connected to the SMS database server.

72) Elevator Access Denials and Grants Report
The Elevator Access Denials and Grants Report shall provide information on all elevator related access denied and granted events including floor selected, time, card reader, badge, and cardholder name.

73) Elevator Dispatching Devices and Terminals Report
The Elevator Dispatching Devices and Terminals Report shall provide a listing of all elevator dispatching devices with the configured terminals.

74) Elevator Floor Assignments to Cardholders Report
The Elevator Floor Assignments to Cardholders Report shall list all cardholders that have access to a particular elevator floor list.

75) Emergency Events Report
The Emergency Events Report shall provide a listing of all emergency events over time.

76) Event Codes Report
The Event Codes Report shall provide information on all event code templates and event code mapping configurations.

77) Event Count by Panel Report
The Event Count by Panel Report shall provide a count of all events grouped by Intelligent System Controller. This report shall include a pie chart breakdown.

80) Fire Device Input or Output Report
The Fire Device Input or Output Report shall provide a listing of all fire inputs and outputs grouped by panel and fire device.

81) Global APB or Mobile Verify Occupancy by Date Report
The Global APB or Mobile Verify Occupancy by Date Report shows the last known area accessed by each cardholder, sorted by date and time.

82) Global APB or Mobile Verify Occupancy by Name Report
The Global APB or Mobile Verify Occupancy by Name Report shows the last known area accessed by each cardholder, sorted by cardholder.

83) Global I/O Linkages Report
The Global I/O Linkages Report shall provide a listing of all global I/O linkages, including the input events and output actions.

84) Guard Tour Configuration Report
The Guard Tour Configuration Report shall provide a listing of all configured guard tours, including checkpoints, actions, and messages.

85) Guard Tour History Report
The Guard Tour History Report shall provide a listing of all events associated with checkpoints that happened for each guard tour.

86) Hardware Panels Report
The Hardware Panels Report shall provide information on all top level hardware panels grouped by category including access panels, fire panels, intercom panels, personal safety panels and central station alarm receivers.

87) Holidays Report
The Holidays Report shall provide information on all system holiday definitions.

88) ILS Lock Authorizations by Cardholder Report
The ILS Lock Authorizations by Cardholder Report shall list ILS lock authorization levels assigned to cardholder/badge, sorted by cardholder.

89) ILS Lock Authorizations by Level Report
The ILS Lock Authorizations by Level Report shall list ILS lock authorization levels assigned to cardholder/badge, sorted by level.

90) ILS Lock Characteristics Report
The ILS Lock Characteristics Report shall list ILS lock configuration details.

91) ILS Lock Communications Report
The ILS Lock Communications Report shall list ILS lock wireless diagnostics.

92) ILS Lock Ownership Report
The ILS Lock Ownership Report shall list ILS locks owned by a cardholder.

93) Intercom Functions Report
The Intercom Functions Report shall provide information on all defined intercom functions.

94) Intercom Stations Report
The Intercom Stations Report shall provide information on all intercom stations, grouped by intercom exchange.

95) Intrusion Command Authority – Advanced Report
The Intrusion Command Authority – Advanced Report shall list all cardholders that have access level assignments configured to use advanced intrusion command authority.

96) Intrusion Command Authority – Global Report
The Intrusion Command Authority – Global Report shall list all cardholders who are assigned access levels with global intrusion command authority.

97) Intrusion Command Events Report
The Intrusion Command Events Report shall list all events associated with intrusion commands including device, cardholder name, and badge.

98) Intrusion Detection Areas Report
The Intrusion Detection Areas Report shall provide a listing of all intrusion areas grouped by panel.

99) Intrusion Detection Devices Report
The Intrusion Detection Devices Report shall provide a listing of all intrusion devices grouped by panel.

100) Intrusion Panel User Groups Report
The Intrusion Panel User Groups Report shall provide a listing of all intrusion user groups grouped by panel.

101) Last Location of Cardholders Report
The Last Location of Cardholders Report shall provide information on the last card reader accessed by each cardholder, sorted by cardholder name.

102) Locked Video Events Report
103) The Locked Video Events Report shall list all system events with associated locked video events.

104) Maps Report
The Maps Report shall provide a list of all available maps in the database.
105) Mobile Verify User Transaction Log Report
The Mobile Verify User Transaction Log Report shall provide a chronological log of all performed transactions.

106) Mobile Verify User Transaction Log by Operation Report
The Mobile Verify User Transaction Log by Operation Report shall provide a chronological log of all performed transactions grouped by operation.

107) Mobile Verify User Transaction Log by User ID Report
The Mobile Verify User Transaction Log by User ID Report shall provide a chronological log of all performed transactions grouped by User ID.

108) Module Details Report
109) The Module Details Report shall provide information about module definitions, grouped by parent panel.

110) Module Summary Report
111) The Module Summary Report shall list all modules, grouped by parent panel.

112) Monitor Stations Report
The Monitor Stations Report shall provide information on all monitoring stations defined in the SMS including which monitor zones and access panels are assigned to the monitoring station.

113) Monitor Zones Report
The Monitor Zones Report shall provide information on all monitor zone definitions.

114) NGP Panels Report
115) The NGP Panels Report shall provide information about NGP Panel definitions.

116) Overdue Visits Report
The Overdue Visits Report shall provide a listing of all scheduled visits that have not signed in.

117) Overstayed Visits Report
The Overstayed Visits Report shall provide a listing of all visitors logged into the facility, but whose badge or visit has expired.

118) Permission Profiles Report
119) The Permission Profiles Report shall provide information on permission profile definitions.

120) Personal Safety Transmitter Assignments Report
The Personal Safety Transmitter Assignments Report shall provide information on all personal safety transmitters and their assignments to cardholders and assets.

121) Personal Safety Transmitters Report
The Personal Safety Transmitters Report shall provide information on all personal safety transmitters.

122) Personnel in the Database Report
The Personnel in the database Report shall provide information on all personnel in the database with basic information.

123) Personnel Without an Active Badge Report
The Personnel Without an Active Badge Report shall provide information on all personnel in the database that do not have an active badge assigned to them.

124) Personnel with Organizational Details Report
The Personnel with Organizational Details Report shall provide information on all personnel in the database with organizational details. This report is designed to work with the SMS standard cardholder layout.

125) Personnel with Personal Details Report
The Personnel with Personal Details Report shall provide information on all personnel in the database with personal details. This report is designed to work with the SMS standard cardholder layout.

126) Point of Sale Registers Report
The Point of Sale Registers Report shall provide a listing of all Point of Sale Registers configured in the SMS.

127) Precision Access Groups Report
The Precision Access Groups Report shall provide information on all precision access group definitions.

128) Reader Assignment to Cardholders Report
The Reader Assignment to Cardholders Report shall provide a listing of all card readers assigned to a cardholder, sorted by cardholder.

129) Reader Command Programming Configuration Report
130) The Reader Command Programming Configuration Report shall list all command programming readers along with the associated user and instant commands.

131) Reader Status Events Report
The Reader Status Events Report shall provide information on card reader status events, grouped by card reader.

132) Reader Timezone Schedules Report
The Reader Timezone Schedules Report shall provide information on all card reader timezone scheduling for card reader modes.

133) Readers Report
The Readers Report shall provide information on all card reader definitions grouped by access panel.

134) Receiver Account Alarm Activity Report
135) The Receiver Account Alarm Activity Report shall provide information on all alarm activity for receiver accounts including notes and elapsed times.

136) Receiver Account Areas Report
The Receivers Account Areas Report shall provide a listing of all receiver account areas, grouped by receiver account.

137) Receiver Account Groups Report
The Receivers Account Groups Report shall provide a listing of all receiver account groups and the receiver accounts contained in each group.

138) Receiver Account Zones Report
The Receivers Account Zones Report shall provide a listing of all receiver account zones, grouped by receiver account.

139) Receiver Accounts Report
The Receiver Accounts Report shall provide a listing of all receiver accounts in the SMS.

140) Receiver Accounts that Failed to Report Report
The Receiver Accounts that Failed to Report Report shall provide a listing of receiver accounts that failed to report during their duration.

141) Receiver and Receiver Account Events Report
The Receiver and Receiver Account Events Report shall provide a listing of all events that occurred on a receiver or receiver account.

142) Segment Badge Download Summary Report
The Segment Badge Download Summary Report shall provide information on each segment by listing the number of badges that must be downloaded to the access panels in that segment. This report shall only work on systems utilizing database segmentation.

143) Segments Report
The Segments Reports shall provide a listing of all segments defined in the SMS along with their options.

144) SNMP Agents Report
The SNMP Agents Report shall provide a listing of all SNMP Agents configured in the SMS.

145) SNMP Management Information Base Configuration
The SNMP Management Information Base Report shall list all MIB data grouped by enterprise.

146) System Servers Report
147) The System Servers Report shall provide a listing of servers defined on the system.

148) Text Instructions Report
The Text Instructions Report shall provide information on all text instructions defined in the SMS.

149) Timezones Report
The Timezones Report shall provide information on all timezone definitions.

150) User Permissions Report
The User Permissions Report shall provide information on all SMS users and their permissions.

151) User Transaction Log Report
The User Transaction Log Report shall provide a chronological log of all transactions performed on the SMS by users.

152) User Transaction Log by User ID Report
The User Transaction Log by User ID Report shall provide a chronological log of all transactions performed on the SMS by users grouped by User ID.

153) Users with Area Access Levels to Manage Report
The Users with Area Access Levels to Manage Report shall list all Area Access Manager users and the access levels that they manage.

154) Video Cameras Device Links Report
The Video Cameras Device Links Report shall provide information on all device links for each video camera.

155) Video Cameras Report
The Video Cameras Report shall provide information on all video cameras grouped by digital video recorder.

156) Video Events Report
The Video Events Report shall provide information on all SMS events with associated video events.

157) Video Servers Report
The Video Servers Report shall provide information on all digital video recorders.

158) Visits History Report
The Visits History Report shall provide information on all visits enrolled into the SMS.

159) Visitors Report
The Visitors Reports shall provide information on all visitors in the SMS.

160) Windows Event Log Errors Report
The Windows Event Log Errors Report shall provide information on all errors logged by the SMS to the Windows event log.

The report user interface in System Administration shall allow the System Administrator to filter on the UTC time columns.

The SMS shall provide filters for each report that, depending on the report that the System Administrator is running, will allow the System Administrator to filter any of the below listed criteria. The SMS shall allow reports to be filtered by any combination of card readers, date and time, cardholder first name and/or last name, area, Action Type, Details or Object, Alarm Acknowledgement and/or badge ID. The SMS will store all reports in the database so that all client workstations will have instant access to the report. The reports shall not be installed in a shared disk directory.

The SMS shall support advanced filters. The SMS shall allow reports to use the Time filter to span across multiple days to create shift reports. For example, a report shall be able to be run that shows all access grants that occurred Monday through Friday, but on during the hours of 8:00 AM to 5:00 PM on those days.

The SMS shall allow for cardholder related reports to be run from the Alarm Monitoring application of the SMS.

When running a report, the SMS shall alert the System Administrator if the report contains deprecated fields.
The current World Time Zone shall display on a report when it is run, along with report date or time.
The SMS shall allow System Administrators to specify card readers as either an ‘in reader’ or an ‘out reader’. The designation of these card readers will act as another filter to use in conjunction with the standard reports to produce ‘raw data’ which shall be exported to external systems such as Human Resources or Excel Spreadsheets which can crunch the data for Time and Attendance purposes.
The SMS reporting interface shall be available from the System Administration Module as well as the Alarm Monitoring application.
The SMS shall support configuring default printers for printing reports.

2. Ad-hoc Database Report Generator
The SMS must provide an ad-hoc customized report generator package integrated with the SMS’s database. This program shall allow the System Administrator to create reports using the relational database structure. Among other reports, a tabular type report shall be configurable which will detail any information from the database in a columnar format with headings, breaks, sub-totals and totals. The report must also be able to be created to produce a flat ASCII export file. Access rights shall be provided to allow the System Administrator the privilege of creating, deleting, updating, saving, processing, viewing and printing reports. The reports are to be printed on a dot matrix printer or on a laser printer. Report configuration shall use menu options and drop-down list boxes to define that database fields are to be used, linked, or joined. They shall also be used to specify conditions and column order, as well as describe the layout and headings.

3. Custom Report Writer
The SMS shall support an industry standard, off the shelf, custom report writer, such as Crystal Reports 11, or 11.5. The custom report writer shall support multiple report types including, but not limited to, multiple section reports, form style reports, conditional reports, query reports, and columnar reports. The custom report writer shall have BLOB Bitmap support and shall come standard with a formula editor with more than 160 built-in functions for System Operators to manipulate data. It shall have export capabilities to ASCII files, Microsoft Mail, or ODBC file formats. The custom report writer shall be compatible with industry standard SQL databases, such as Microsoft SQL Server 2005 or Microsoft SQL Server 2008.

4. System Tape Backup
A mandatory requirement, the SMS shall provide tape backup and restore programs utilizing the multi-tasking capabilities of the SMS and operating system. These programs shall run concurrently with any other application. Database backup must occur dynamically while other alarm monitoring, badging, access control applications remain active.
The tape backup feature shall allow for three levels of tape backup; 1) Incremental, which will back up to tape all changes to data and images that have changed since the last incremental tape backup, 2) System, which will back up the operating system and application files only, and 3) Full, which back ups all files.
A database snapshot shall occur prior to a tape backup and the actual backup shall be performed in the background, utilizing the benefits of the multi-tasking operating system, without interfering with the ability of System Operators to exercise other functions.

5. Client workstations
System Administrators shall have the ability to configure each client workstation on the SMS to utilize any combination of event printers, CCTV controllers, and video capture boards. For each printer or CCTV controller, System Administrators shall be able to select the port that the device is connected to on the client workstation and the communications speed.

6. PIN Numbers
The SMS shall have the ability to support up to nine (9) digit PIN Numbers for each cardholder in the SMS. PIN Numbers shall be created either manually through System Operator entry or generated randomly by the SMS. The SMS shall have the ability to be
configured to allow for unique PINs for each cardholder and the ability to modify cardholder’s PIN numbers at a later date.

7. List Builder
System Administrators shall have the ability to pre-define information that will appear in each of the pre-defined drop-down lists. There shall be no limit to the number of items that shall be a part of a list. Lists can have items added to them or deleted from them at any time.

8. Archiving
The SMS shall allow System Administrators to archive offline history files to magnetic media. Offline files shall include access events and System Operator transactions that have been purged from the reportable database. The offline files MUST be in a “ready to import” format for easy insertion of information back into the online database. Different event types may remain in the database for different time periods according to the System Operator's specification.

Any record older than the specified dates shall be purged to the offline history file for archiving. Reports shall be generated from the archived files if necessary. Archiving shall be a scheduled, automatic function.

9. Remote Dial-In Capabilities
The SMS shall support remote dial-in capabilities for SMS troubleshooting, SMS configuration, and alarm monitoring capabilities.

VAR and/or System Administrators shall be able to dial in to the CUSTOMER database server to troubleshoot the CUSTOMER's system. This will allow System Administrators to locate any problem areas and, many times, fix the error over the telephone from a remote location.

Remote dial-in shall also be used for SMS configuration and/or alarm monitoring from remote locations using a client workstation. The client workstation shall have the ability to operate on a Laptop PC that meets the client workstation minimum specifications.

10. Reader Groups
a. The SMS shall support reader groups. The SMS's Grouping form shall be used to:
   1) Specify the group or groups to which the reader belongs.
   2) Search for readers by group (The search for readers button is available from all of the forms in the Readers folder.)
   3) Name and save lock group search criteria for future use.

b. Six (6) default reader group drop-downs are provided on the SMS’s Grouping form.

11. Mobile Enterprise Applications: This section is designed to be utilized in addition to, and in conjunction with, the rest of the SMS Functional Generic Specification. It is designed for use with those systems that deploy, or wish to deploy, the SMS Mobile Enterprise Architecture for Mobile Computing requirements.

The Mobile Enterprise Architecture is a mobile, synchronized database solution that is designed for customers with mobile computing needs. Mobile Enterprise functionality shall be a seamlessly integrated, robust solution that transports virtually all SMS client functions to a wearable, portable computer that connects to the network and SMS Server via 802.11b wireless Ethernet online, or as a standalone solution that can be synchronized with the SMS Server on an operational basis.

At a high level, Mobile Enterprise shall offer:

a. Wearable computers for mobile computing applications
b. Standard SMS software
c. Wireless network connectivity
d. Standalone operations
e. Central Database Storage Facilities
f. Data Synchronization Between Multiple Databases
g. Mobile Alarm Monitoring and System Administration Capabilities
h. Unlimited Expansion Capabilities
i. Open Architecture Design
j. Advanced Network Design
k. Integration with Digital Video, ID Credential Management, and Visitor Management Systems

12. The SMS shall support a multi-PC, multiple database synchronization architecture (herein after Mobile Enterprise Architecture) using a database server. The database server shall allow multiple wearable or mobile computers to be connected to it (via wired or wireless LAN or WAN architecture). In a stand-alone environment, connections shall occur only during synchronization.

13. The database server shall contain a master copy of all relevant system data. An unlimited number of mobile enterprise client workstations may be connected to the database server.

14. In a stand-alone environment the mobile enterprise computing PC shall contain a copy of all required core information obtained from the database server. This shall include, but not be limited to, cardholders, badges, badge types, and access permissions.

15. At predetermined, user-definable, periodic intervals, each of the stand-alone mobile enterprise computers shall connect to the database server to perform a database synchronization process.

16. In a wireless, online environment during daily SMS operation, each of the mobile enterprise client workstations shall be connected locally to the database server via industry standard 802.11b wireless network connectivity. Mobile enterprise client workstations shall be any combination of system administration, alarm monitoring, digital video, visitor management, remote access level management, or ID management applications.

17. Unlimited system expansion and scalability shall be possible with the Mobile Enterprise architecture. There shall not be a limit to the number of mobile enterprise computing PCs that can be deployed.

a. Application Support
   Mobile Enterprise shall support any SMS application on its mobile computing platform including:
   1) Access Control
   2) Alarm Monitoring
   3) ID Credential Management
   4) Digital Video
   5) Intrusion Detection
   6) Visitor Management

b. Platform Support
   Mobile Enterprise shall be deployed onto a mobile PC computing platform. Minimum mobile computing platform specifications shall be as follows:
   1) Operating System: Microsoft Windows 7 or 2008 or 2003 or XP or Vista
   2) Processor: 600 MHz Transmeta Crusoe™
   3) Size: 9.75 in. (L) x 3 in. (W) x 1.25 in. (D) (24.76 cm (L) x 7.62 cm (W) x 3.17 cm (D))
   4) Weight: 22 oz (624 grams)
   5) RAM: 128 MB DRAM
   6) Hard Drive: 6 GB or greater
   7) PC Card slots: Two Type II or one Type III
   8) Temperature Range: 32 degrees F to 122 degrees F (0 degrees C to 50 degrees C)
   9) Battery: Lithium Ion, Hot-Swappable
   10) Run time: 7 to 12 hours on a two-battery system
   11) Display: SVGA Indoor or Outdoor glass with Magnesium case

c. Mobile Verify
   Mobile Enterprise shall support a Mobile Verify software option specifically designed for Mobile Enterprise Solutions, which shall provide the ability for an officer to use an optional scanner or card reader to automatically search the database for access privileges. The officer shall instantly be presented with the answer of either Access
Granted or Access Denied based on the credential holder’s privileges. This functionality shall be accomplished in either standalone or online mode.

d. Network Connectivity
Mobile Enterprise shall be deployed using industry standard 802.11b wireless network technology. With its high throughput and long range, 802.11b shall operate in the unlicensed 2.4GHz frequency spectrum that is well established in corporate wireless markets.

e. Stand-alone Mode
Mobile Enterprise shall also be deployed as a stand-alone mode. In a stand-alone environment the mobile computing PC shall contain a copy of all required core information obtained from the database server in order to execute Mobile Verify functionality. This shall include, but not be limited to, cardholders, badges, badge types, and access permissions.

f. Login Privileges
Any mobile enterprise client workstation shall have the ability to log into the system for the purpose of System Administration, Alarm Monitoring, ID Credential Management, Mobile Verify, etc.
The System Administrator or System Operator at the mobile enterprise client workstation will have appropriate privileges based on their login ID and permissions for that particular user account as determined on the database server.

g. User Transactions
User transactions shall be logged on all mobile enterprise computing clients and shall be stored at the database server.

18. Badge Layout Creation Module: The SMS shall provide a Badge Layout Creation and Editing Module to allow for the creation of custom badge designs to be created by the CUSTOMER. The SMS shall support credit card, government, and custom credential sizes in either a landscape or portrait format.

a. Badge Layout Objects
The SMS shall support multiple object types, all of which shall be placed on the layout in any order and combination. These objects shall include alphanumeric text fields, database fields, photos, signatures, logos, graphics, shapes (square, circle, rectangle, ellipse), and bar codes. Objects shall be placed onto the layouts through a Windows drag and drop process.

b. Advanced Database Field Driven Badge Layouts
The SMS shall support advanced functionality that allows cardholder database information to control what information is printed onto a cardholder’s credential. Thus, a single generic layout shall be created, and attributes such as colors, borders, logos, typefaces, backgrounds, etc. shall be determined by the information of a particular database field. For example, when ‘Marketing’ is entered in the Department field, a green background shall be printed on the badge. However, when ‘Engineering’ is entered in the Department field, a blue background shall be printed on the badge.

Any information displayed in a drop-down list shall have the ability to control any of the following credential attributes:
The SMS shall support insertion of extended ASCII codes into the Text property of objects within the badge layout.

c. Object Properties
System Administrators shall have the ability to edit each object placed onto the layout using a ‘Properties Form’ to customize each object on the layout.

1) Text and Database Objects
System Administrators shall be able to adjust the positioning of the object, its height and width, along with the object’s color and color fill style (solid, horizontal lines, etc.). Borders (if any), along with the border width and border style shall also be modifiable. The typeface of any text shall be user-definable (font, size, bold, italic, underline) as well as the alignment of the text inside of the object (left, center, right, top, middle, bottom).
System Administrators shall be able to allow word wrapping of text within the object and shall be allowed to set the maximum number of characters allowed in the object.

2) Photo, Signature, and Graphic (logo) Objects

System Administrators shall be able to adjust the positioning of the object, its height and width, along with the object's color and color fill style (solid, horizontal lines, etc.). Borders (if any), along with the border width and border style shall also be modifiable. Attributes shall be available for auto sizing and scaling the photo, signature, or graphic that shall be located in the object. Keeping aspect ratio shall be an option. Alignment of the photo, signature, or graphic inside of the object (left, center, right, top, middle, and bottom) shall be available. System Administrators shall also be able to chromakey and/or ghost the photo or graphic. System Administrators shall also be able to tile the image or logo in any number of rows and columns across the background of the credential.

3) Shape Objects

System Administrators shall be able to adjust the positioning of the object, its height and width, along with the object's color and color fill style (solid, horizontal lines, etc.). Borders (if any), along with the border width and border style shall also be modifiable. System Administrators shall have the option of inserting square, circle, rectangle, or ellipse shapes.

4) Bar code Objects

System Administrators shall be able to adjust the positioning of the object, its height and width, along with the object's color and color fill style (solid, horizontal lines, etc.). Borders (if any), along with the border width and border style shall also be modifiable. System Administrators shall have the ability to rotate the bar code to a vertical or horizontal position on the layout. The SMS shall allow System Administrators to encode any database field and/or other information onto the bar code, depending on the bar code type selected.

5) Object List

An object list shall be available to System Operators to allow them to select objects without clicking on them in the layout with the mouse. This shall be helpful when one object has been placed onto top of the other, making it difficult to select the object in the background with the mouse; or when System Operators wish to select an object without moving the object's position on the layout.

6) Color Palette

The SMS shall support a Windows Color Palette capable of creating up to 16.7 million colors to be used in applying color to the various objects, shading, and/or borders in the badge layout.

7) Import of Badge Layouts

The SMS shall also allow for the importing of badges from a .bdg file.

8) Multiple Badge per Page Printing

The SMS shall allow for System Operators to print multiple badges to the same page. System Administrators can configure the SMS to print multiple badges to a pre-defined number of columns and rows to accomplish 2 up, 4 up, 6 up, or 8 up printing. This feature is useful when printing badges for visitors.

9) Working with Objects

A set of alignment tools shall be available to System Administrators to manage objects. ‘Move to Front’, ‘Send to Back’, ‘Move Forward’, and ‘Move Backward’ commands shall be available to allow objects to be placed on top of other objects. The SMS shall support the rotation of objects in 90 degree increments (0 degrees, 90 degrees, 180 degrees, 270 degrees).

A zoom command shall be available to allow System Administrators to manage the layout in multiple views. User-definable sample field data shall be available for ease of working with objects. When objects are placed onto a layout, the sample data will fill in to show the System Administrator what effect the object has on the layout.
System Administrators shall also be able to select the color of the PVC card that they are working with so they will see the effect that it has on the layout. They shall also be able to place the magnetic stripe outline on to the layout for ease of aligning other objects. All Badge Layouts shall be placed in a gallery for previewing.

19. Screen Designer Tool

a. SMS Cardholder Standard Fields and Objects

The SMS shall support at a minimum the following standard fields for personnel information:

1) Last Name
2) First Name
3) Middle Initial
4) Social Security Number
5) Badge Type
6) Address 1
7) Address 2
8) City
9) State
10) Zip Code
11) Phone Number
12) Birth Date
13) Title
14) Department
15) Division
16) Location
17) Building
18) Floor
19) Office Phone Number
20) Extension
21) Signature
22) Last Reader Accessed
23) Record Last Changed
24) Badge ID
25) Issue Code
26) Number of Prints
27) Activation Date
28) Deactivation Date or Time
29) Badge Status
30) PIN Number
31) Embossed Number
32) Date of Last Badge Print
33) Photo
34) Photo Display

b. SMS Asset Standard Fields and Objects

SMS shall support at a minimum the following standard fields for asset information:

1) Scan ID
2) Asset Name
3) Acquired
4) Replace
5) Type
6) Subtype
7) Serial Number
8) Department
9) Assessed Value
10) Replacement Value
11) Last Inspection
c. SMS Visitor Standard Fields and Objects

SMS shall support at a minimum the following standard fields for visitor information:

1) Last Name
2) First Name
3) Middle Initial
4) Badge Type
5) Organization
6) Title
7) Address 1
8) Address 2
9) City
10) State
11) Zip Code
12) Office Phone
13) Extension
14) Last Changed
15) Last Reader Accessed
16) Record Last Changed
17) Badge ID
18) Issue Code
19) Number of Prints
20) Activation Date
21) Deactivation Date or Time
22) Badge Status
23) Photo
24) Photo Display

d. SMS Visit Standard Fields and Objects

1) Host Name
2) Visitor Name
3) Status
4) Scheduled Time In
5) Scheduled Time Out
6) Actual Time In
7) Actual Time Out
8) Last Changed
9) Type
10) Purpose

e. User-definable Fields

Should the SMS standard fields not be suitable, System Administrators shall have the ability to modify any standard field to customize the cardholder, asset, and visitor forms as desired. The SMS shall also allow System Administrators to add custom fields in addition to or replacement of any standard fields on a minimum of thirty two (32) pages each of information for the cardholder, visitor, and visit forms and one page of information for asset. User-defined fields absolutely shall not be pre-defined, meaning only the labels can change while the properties cannot. System Administrators shall have a minimum of sixteen pages of which to design their screens with standard and custom fields.

f. System Administrators shall have the ability to modify the pages of information in any combination as follows:

1) Move standard database fields to different locations on the cardholder forms
2) Delete standard database fields that are not desired
3) Keep standard database fields in the same location as the factory ships them, but changing the label and/or any field attributes. For example, Zip Code may be changed to Postal Code and the attributes changed from a number field to text field for Canadian installations
4) Add new fields to the cardholder forms each with their own unique set of attributes

g. Field Types
The SMS shall support, at a minimum, the following field types:
1) Text Fields
2) Date Fields
3) Numeric Fields
4) Drop-down Lists

h. Field Attributes
System Administrators shall be able to assign any combination of the following attributes to each field defined:
1) Positioning of the field on the form
2) From which page the field can be viewed
3) From which page the field can be edited
4) The font to be used for the information that will appear in the field. The SMS shall support all standard Windows fonts
5) The style to be used for information that will appear in the field. The SMS shall support bold, italic, both, and regular typeface styles
6) Any effects to be used for the information that will appear in the field. The SMS shall support strikeout and underline
7) Whether the field is required
8) Whether the field is to be indexed
9) Whether the field is unique
10) If a template is to appear in the field
11) If a default value will appear in the field

i. Field Styles
System Administrators shall be able to assign any combination of the following styles to each field defined:
1) Multi-line field
2) Horizontal Scroll
3) Vertical Scroll
4) Auto Horizontal Scroll
5) Auto Vertical Scroll
6) Enter means next line of text
7) Number
8) Uppercase
9) Lowercase
10) Read Only
11) Align Right
12) Password
13) Sunken
14) Border
15) Inside Edge
16) Raised
17) OEM Covert

j. Field Alignment and Width Tools
The SMS shall support the following field alignment tools to allow System Administrators to align fields and set uniform widths to fine tune the look and feel of the screens. The SMS shall allow System Administrators to select multiple objects simultaneously and
align them to their desired position and/or set a uniform width. The following field alignment tools shall be able to be used in any combination:

1) Align all objects selected to the far left edge of the farthest left selected object
2) Align all right edges of selected objects to the right edge of the farthest right selected object
3) Align the tops of all selected objects to the top edge of the highest selected object
4) Align the bottom edges of all selected objects to the bottom edge of the lowest selected object
5) Align all selected objects to be vertically centered with respect to each other
6) Center all selected objects
7) Make all selected objects the same width as the smallest object selected
8) Make all selected objects the same width as the widest object selected
9) Make all selected objects the same height as the shortest object selected
10) Make all selected objects the same height as the tallest object selected
11) Evenly space all objects vertically between the two most outer objects
12) Evenly space all objects horizontally between the two most outer objects
13) Bring object to the front of the page
14) Send object to the back of the page

k. Tab Ordering
The SMS shall allow System Administrators to set the TAB order (the order in which the cursor moves throughout the fields) of the SMS when System Operators utilize the TAB key to move throughout the cardholder form.

20. Map Editor Module
The SMS shall support graphical map creation software that shall allow the import of map backgrounds from any standard ‘off-the-shelf’ drawing package in the formats listed below:

a. AutoCAD DXF (.dxf)
b. Bitmaps (.bmp, .dib)
c. JPEG (.jpg)
d. JIFF (.jif)
e. Zsoft PCX/DCX (.pcx, .dcx)
f. Adobe Photoshop (.psd)
g. CALS Raster (.cal)
h. GEM/Ventura IMG (.img)
i. IBM IOCA (.ica)
j. WordPerfect Raster (.wpg)
k. Macintosh PICT (.pct)
l. Portable Network Graphics (.png)
m. TIFF (.tif)

These architectural type maps must allow the detailed layout of an entire structure, part of a structure, a floor or department within a building, or layout of the periphery of a facility. Once a map has been drawn, the System Administrator must have the ability to place system level icons of card readers, input and output points, video cameras, and other access control field hardware 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 must allow various maps to be associated with each area to provide for the creation of hierarchy of maps. Overview maps of an entire facility shall be able to be
viewed as requested and nested maps shall be accessed from the overview map to enlarge a specific area or facility on the screen. Maps shall also support user-defined text that shall be placed onto the map background.

The SMS shall allow hardware device icons to be either static or part of a device group. Icons that are part of a device group shall allow the hardware device icon to change shape and/or color based on the current state of the device.

Maps shall have the ability to be printed and/or previewed from the Map Editing Module or the Alarm Monitoring application.

The SMS shall also support custom device icons to be used with the maps (.ico) files.

21. Import Module: The SMS shall support an import utility, which shall allow the CUSTOMER or VAR to import cardholder information into the SMS database. This shall allow the CUSTOMER or VAR to pre-populate the SMS database with existing cardholder data and/or add NEW records to an existing SMS database. The Import Module only supports SQL Server; it does not support Oracle. For Oracle, DataExchange must be used for data import.

The Import Utility shall be a 32-bit Windows application that shall be used to import standard ASCII delimited text files into the SMS. The import utility shall be utilized at the initial SMS setup and anytime a large number of records need to be imported into the SMS after the initial import. For example, a large university may import 10,000 records into the SMS during the initial SMS setup and then import 2,000 additional records each semester thereafter. The SMS shall check for duplicate records during the import, so that multiple copies of the same record are not added into the SMS database.

The import utility shall allow System Administrators to choose the delimiter for the ASCII file. This delimiter may be, but is not limited to, a comma, vertical bar, semi-colon, or asterisk. Fields in the SMS database, such as Address 2, that the CUSTOMER does not wish to use, may be left blank in the ASCII file.

The import utility shall be able to select the source drive where the ASCII delimited file is located as well as the destination drive where the SMS database is located.

The import utility shall also be able to import photos as part of the record into the SMS database. The SMS shall support the following file formats for the import of cardholder photos:

a. Bitmaps (.bmp, .dib)
b. JPEG (.jpg)
c. JIFF (.jif)
d. Zsoft PCX/DCX (.pcx, .dcx)
e. Adobe Photoshop (.psd)
f. CALS Raster (.cal)
g. GEM/Ventura IMG (.img)
h. IBM IOCA (.ica)
i. WordPerfect Raster (.wpg)
j. Macintosh PICT (.pct)
k. Portable Network Graphics (.png)
l. TIFF (.tif)
m. Windows Metafile (.wmf, .emf)
n. Targa (.tga)
o. Kodak Photo CD (.pcd)
p. Kodak Flashpix (.fpx)
q. Encapsulated Post Script (.eps)

The SMS shall include a progress meter to show the System Administrator the percentage of the import complete when importing large quantities of records.

22. DataExchange: The SMS shall support an import or export utility that shall enable advanced System Administrators to import data and images into the SMS database and export data and images from the SMS database for use with third-party software systems.
The DataExchange Utility shall allow for bi-directional communications with external systems. It shall allow for the import into the SMS database and the export out of the SMS database personnel information, including images, through ASCII delimited files or XML files.

The import or export scripts shall run on schedule and shall be accomplished over the network. DataExchange is ideal for customers who wish to have a base line level of integration with third-party external systems such as those used for Time and Attendance and Debit Card systems. Database import and export scripts shall be stored in the SMS database. A user interface shall allow for the generation of import and export scripts. When configuring or running a DataExchange script, the SMS shall alert the System Administrator if deprecated fields are being used.

The file used for import or created by export shall have the ability to be structured in a wide variety of ways, but shall always be in either ASCII text, Unicode text, XML, or Database format. System Administrators can configure the import procedures to put the new data into any of the tables of the SMS database. As such, export data shall be taken from any tables in the SMS database.

a. File Imports
DataExchange shall allow data to be imported into the SMS database. Importing of information shall occur in one or more of the following methods:

1) Add - The data in the file shall be added to the database. If a particular record is already in the database, an error shall occur and the record shall be rejected and placed in an error log.

2) Change - If a record in the file exists in the database, the record shall be modified according to the layout configuration specified. Records in the file that don’t already exist in the database shall be rejected and placed in an error log file.

3) Delete - If a record in the file exists in the database, it shall be deleted.

4) Add or Modify - If a record in the file exists in the database, it shall be replaced according to the layout configuration you specified. Records that don’t already exist shall be added to the database.

b. DataExchange shall support a minimum of the following image file formats to be imported into the SMS database:

1) Adobe Photoshop 3.0 (PSD)
2) CALS Raster (CAL)
3) Delrina WinFax Group 3 (FAX)
4) Delrina WinFax Group 4 (FAX)
5) Encapsulated PostScript (EPS)
6) FAX Group 3 (FAX)
7) FAX Group 4 (FAX)
8) GEM Image (IMG)
9) IOCA or IBM Image Object Content Architecture (ICA)
10) JIFF or JPEG File Interchange Format (JPG or JIF)
11) JPEG Tagged Interchange Format (JTIF)
12) Kodak FlashPix (FPX)
13) Kodak PhotoCD (PCD)
14) LEAD CMP (CMP)
15) Macintosh Pict Format (PCT)
16) MacPaint (MAC)
17) OS/2 Bitmap (BMP)
18) Portable Network Graphics (PNG)
19) SUN Raster Format (RAS)
20) Truevision TARGA (TGA)
21) Microsoft Paint (MSP)
22) Windows Bitmap (BMP)
23) WordPerfect Format (WPG)
24) Zsoft PCX/Multipage PCX (PCX/DCX)
DataExchange shall utilize an error log that shall report all errors that occur during a file import. Any and all errors can then be viewed from this log, corrected, and the import shall run a second time to download the corrected records.
DataExchange must allow imported changes to be downloaded to Intelligent System Controllers on a near real-time basis as information is being imported into the database.
c. Exporting Data
DataExchange shall allow data to be exported from the SMS database. Any combination of SMS database fields shall have the ability to be exported to a Database or Unicode text file.
d. Data Expressions
DataExchange shall support run-time data generation to support customer business logic. Following expression types shall be provided:
1) Constants
This type of expression shall provide import or export with data that doesn't change like "5" or "Employee". The System Administrator shall configure the value. Constant expressions shall be able to be parts of other expressions.
2) Increments
Similar to numerical constants, but changes as import or export progresses. For example: "1" for the first record, "3" for the second, "5" for the third etc. The System Administrator shall configure a base value ("1" in example) and increment ("2" in example).
3) Lookups
Lookup expressions query the SMS database with System Administrator provided data and return query result. For example, System Administrator data contains a department name such as "Engineering", but to import a record department ID is needed. The System Administrator shall configure a lookup on DEPT table with NAME as a source field and ID as a return field. So lookup with "Engineering" will return "2". Lookup expressions shall be cascaded or be parts of other expressions (such as conditional expressions). Lookup expressions shall be user configured to add records to a lookup table if value is not found.
4) Conditional expressions
Conditional expressions evaluate a comparison between two pieces of data to either a true or false result, and based on that result return one or the other configured user data. Conditional expressions can be cascaded or be parts of other expressions (such as lookup expressions).
An example of an expression returning file data would be something like the imported data wants to use the default badge type business rule for the deactivate date when adding a new badge. However, if a badge already exists for the cardholder, use it's deactivate date.
e. Import or Export Filters
The DataExchange shall allow System Administrators to select a subset of data for export or database import operations. SQL filter shall be used do define which records would be selected for the import or export.
23. SMS Server Redundancy
a. The SMS shall support multiple levels of fault tolerance and SMS redundancy listed and described below:
1) Hot Standby Servers
2) Clustering
3) Disk Mirroring
4) RAID Level 10
5) Distributed Intelligence
b. Hot Standby Server Solution
The SMS shall support a fault tolerant server and redundant database architecture. It shall allow for normal operations to occur in the event that the Database Server fails. In
the event of a server failure, the switch over to a backup server shall be automatic. System Operator intervention for switch over shall not be acceptable.
The SMS shall utilize two servers, which shall be configured identically. One server shall be designated as the Primary Server and the other shall be designated as the Backup Server. The Primary Server shall be the main server that is in use when the SMS is operating under normal conditions.
The SMS shall mirror the database information from the Primary Server to the Backup Server. This mirroring shall be conducted through standard local area network (LAN) communications. There shall absolutely not be any proprietary communication links between the Primary and Backup Servers.
All access control field hardware shall be configured for both the Primary Server and the Backup Server. Both the Primary and Backup Servers shall recognize the same TCP/IP ISC address on the network.
If the Backup Server is not running or receiving the mirrored files from the Primary Server, the Primary Server shall save the changes locally. Upon restored communications to the Backup Server, this information shall be automatically sent to the Backup Server.
In the event that the Primary Server fails, the Backup Server shall sense that the Primary Server has failed and is no longer on the network. The Backup Server shall check to see if the Primary Server is online every five seconds.
Upon sensing Primary Server failure, the Backup Server shall automatically initiate itself as the Primary Server and shall begin communication with the Intelligent Fields Panels. ABSOLUTELY NO SMS OPERATOR INTERVENTION SHALL BE REQUIRED. A message shall be broadcast to all client workstations on the network that the Primary Server has failed and the Backup Server has taken control. This process shall take no longer than two minutes to accomplish.
Once the Primary Server comes back online with the SMS, the Primary Server and Backup Server shall be able to be re-synchronized though automatic operation and resume normal operations. The synchronization process shall be fast, efficient, and take no more than five minutes.
c. Clustering
The SMS shall support a fault tolerant cluster server architecture. It shall allow for normal operations to occur in the event that the Database Server fails. In the event of a server failure, the switch over to a backup server shall be automatic. System Operator intervention for switch over shall not be acceptable.
The SMS shall utilize two servers, which shall be configured identically. One server shall be designated as the Primary Server and the other shall be designated as the Backup Server. The Primary Server shall be the main server that is in use when the SMS is operating under normal conditions.
The SMS shall use shared-media technology. This shall incorporate a third piece of hardware (for example: Dell PowerVault), which shall house the hard disk to be referenced by both servers. Since accessible media is dependent upon a third piece of hardware, emphasis shall only be placed upon the health status of the shared-media device. If the status of the shared-media device remains healthy, server up time is of no consequence to data integrity.
The shared-media device provides only a single point of failure. If this device fails, then data cannot be accessed. A dual point of failure shall be achieved by incorporating two shared-media devices that are mirrored (for example: two stacked mirrored Dell PowerVaults).
All access control field hardware shall be configured for both the Primary Server and the Backup Server. Both the Primary and Backup Servers shall recognize the same TCP/IP ISC address on the network.
In the event that the Primary Server fails, the Backup Server shall sense that the Primary Server has failed and is no longer on the network. The Backup Server shall check to see if the Primary Server is online every 5 seconds.
Upon sensing Primary Server failure, the Backup Server shall automatically initiate itself as the Primary Server and shall begin communication with the Intelligent Fields Panels. ABSOLUTELY NO SMS OPERATOR INTERVENTION SHALL BE REQUIRED. A message shall be broadcast to all client workstations on the network that the Primary Server has failed and the Backup Server has taken control. This process shall take no longer than 2 minutes to accomplish.

Once the Primary Server comes back online with the SMS, the Primary Server shall resume normal operations.

d. Disk Mirroring
The SMS database server shall protect data against failure of a hard disk or hard disk controller by providing a disk mirroring configuration. The disk mirroring configuration shall allow data to be stored on dual hard disks running simultaneously. When any client workstation or Intelligent System Controller sends data to the database server, it shall be stored to both sets of hard disk drives. In the event any component on one channel fails, the other disk drive continues to operate without data loss or interruption. The SMS shall also send a warning message indicating that one disk drive has failed.

e. RAID Level 10
The SMS shall offer a Fault Tolerant Redundant Array of Independent Disks Level 10 (RAID Level 10) with a hot standby disk. RAID Level 10 shall provide redundancy of disk storage, controller channels and power supplies. Each array must contain a disk drive, high efficiency power supply, and cooling fan. This technology shall use multiple drives to store data with distributed parity, thereby ensuring data protection in an environment in which data is safe and easily restorable in the event of a hard disk failure. In the event a single drive within the array fails, a "Hot Standby Hard Disk" shall be available online and automatically switched with the failed unit.

The network administrator shall be able to replace the failed drive without taking the database server down, and it shall then become the hot standby. The array software shall rebuild the lost data from parity information stored on the other drives in the array. This entire procedure shall have no effect on the operation of the SMS and shall be automated.

f. Distributed Intelligence
In the event SMS communications is lost or the database server fails, Intelligent System Controllers shall provide complete control, operation and supervision of all monitoring and control points. The ISC shall be configured with a UPS battery, which shall support the ISC for a 24 hour duration. The ISC shall be installed with enough memory to support up to 100,000 cardholders/100,000 events in a minimum configuration and be expandable to up to 250,000 cardholders/1,000,000,000 events.

The SMS shall incorporate performance tests and precautions so as to avoid SMS failure. In the event of a failure, transactions are to be stored in an ISC First In First Out (FIFO) buffer until the ISC comes back online, at which time all data is uploaded to the database server. The ISC shall register as online with the database server when communications are re-established. Should the ISC buffer fill and events are overwritten, an event will appear in the Main Alarm Monitoring Window notifying the System Operator that events were overwritten. The ISC shall send a time/date stamp of the last record or table update in its memory and request any new data changes or cardholder records which have changed since that time or date stamp. A complete download of database and access tables shall not be required because of offline operation.

24. DataConduIT: The SMS shall allow, through standard API toolkits, System Administrators to expose specific SMS data and events that are relevant to IT information or other third-party systems. Conversely, the SMS shall allow, through these same API toolkits, System Administrators to accept and process information exposed from the IT information or other third-party systems. This shall permit System Administrators to develop scripts and applications that allow events in either the IT domain to cause appropriate actions in the Security domain, and vice versa.

Using the toolkit, the following shall be a sample of the integration opportunities available:
a. When a cardholder account is created in the SMS, DataConduIT shall create a Windows 7 or 2008 or 2003 or XP Active Directory Account for that person. The Windows account name shall be derived from the SMS cardholder name. The SMS account and the Windows account shall then be linked to the same person.

b. When a user’s Windows 7 or 2008 or 2003 or XP Active Directory Account is created, DataConduIT shall create a SMS cardholder account, badge, and access rights. The SMS account and the Windows account shall then be linked to the same person. A cardholder’s phone number changes in the SMS. The new phone number shall be propagated through DataConduIT to the associated user account in the company’s Active Directory.

c. When a cardholder’s access badge is disabled, DataConduIT shall automatically disable that cardholder’s other IT user accounts.

d. Conversely when a user’s Windows or other Active Directory or LDAP account is disabled, DataConduIT shall deactivate the cardholder’s access badge in the SMS.

e. A user’s Windows account for PCs in a research lab is normally deactivated. When a cardholder cards into the research lab, DataConduIT shall activate the user’s Windows account for the computers in the research lab.

f. A third-party system acknowledgment of pending alarms in the SMS database. All business rules pertaining to cardholders, badges, access levels, and linked accounts shall be enforced when a cardholder, badge, access level, or linked account is added, modified, or deleted. Clients shall not be able to make any writes that would be invalid if made through the SMS’s System Administration module.

g. SMS API Toolkit Operations
   1) Operations
      DataConduIT clients shall be able to add new cardholders and modify or delete existing cardholders, visitors, visits, biometrics, and images.
      DataConduIT clients shall be able to add new badges and modify or delete existing badges.
      DataConduIT clients shall be able to add and delete linked accounts. Modification of existing linked accounts shall not be permitted.
      DataConduIT clients shall be able to view directory definitions. Modification of existing directories shall not be permitted.
   2) Software Events
      DataConduIT clients shall be able to register to receive notification when any of the following software events takes place:
      a) A person is added, modified, or deleted (including the person primary segment assignment)
      b) A badge is added or deleted, or its badge status changes
      c) A linked account is added or deleted
   3) Hardware Events
      DataConduIT clients shall be able to register to receive notification when any access control field hardware events take place.
      This shall include access to areas, elevator readers, and assets, and for access attempts under duress.
      This shall include the acknowledgment of pending alarms in the SMS database.

h. Accepting Custom Incoming Alarms and Events
   The SMS shall accept generic or custom incoming events from third-party systems to be displayed in the Main Alarm Monitoring Window, similar to other SMS alarms. In addition, it shall be possible to configure where to route these alarms.
   The SMS shall allow the Main Alarm Monitoring Window to represent the following:
   1) Source – a text representation of the object or device that generated the event
   2) Date or Time – the date and time when the event occurred
   3) Description – text of up to 80 characters that describes the event
4) Additional Text—additional text of up to 1,000 characters associated with the event

i. DataConduIT Devices and Sub-Devices
The SMS shall be able to support downstream devices and sub-devices through DataConduIT. The configuration for these devices shall occur in the DataConduIT Source folder in System Administration.

j. Event Generation with Devices and Sub-Devices
The SMS shall be able to generate Access Granted and Access Denied events from a DataConduIT source, Device, or Sub-Device. The SMS shall also be able to pass the badge identification number along with the access granted or denied. This shall report to the DataConduIT source.

25. Open Protocol Interface

a. The SMS shall provide a set of standard Application Programming Interfaces (API's) and supporting documentation that allows hardware manufacturers and software application developers to interface their products into the SMS. The Application Programming Interfaces shall allow requests to occur from CUSTOMER to interface a third-party hardware or software solution based on SMS open architecture and SMS device independence.

b. There shall be two components to the Application Programming Interfaces. There shall be a device interface and an application interface.

c. The device interface shall allow extensibility to the number and types of hardware devices supported by the SMS. Each individual piece of hardware shall have its own “driver” that shall understand how to communicate with the SMS hardware. These “drivers” or "device translators" shall translate a set of generic commands into specific device commands.

d. The device translators shall be implemented as COM (Component Object Model) objects so that they shall be loaded and unloaded as needed. Each device translator shall support certain interfaces that support a specific set of commands or methods. Some examples of typical interfaces could include an Access Control Interface for access control hardware, a Video Interface for DVR and NVR hardware, an Intercom Interface for intercom systems, an Intrusion Interface to support alarm inputs, etc. A particular device translator shall support many interfaces.

e. The main application that shall be used to control the various device translators is the SMS Communication Server (SCS). The SCS shall be the application that manages and sends the commands to the device translators. Other modules including Alarm Monitoring or System Administration shall communicate with the hardware devices by sending commands to the SMS Communication Server, which shall then send the commands on to the correct device or devices.

f. The device interface shall allow the software interface of any hardware device to be controlled and monitored via the SMS Alarm Monitoring application. This shall preserve customer investments in existing equipment as well as allow for system expansion to occur through the interface of the latest hardware technologies.

g. The application interface shall allow information to be exchanged between the SMS and other applications. The application interface shall provide the functions for interacting with the SMS. This includes the ability to extract information from the SMS database as well the ability to download, control and monitor information for all field hardware including access control panels, digital video systems, fire panels, alarm panels, intercom system, etc.

h. All functions of the application interface shall be defined in such a way that any Windows application or development environment with the ability to make “C” calls should be capable of making use of the API.

26. Open Supervised Reader Interface

a. The SMS shall provide connectivity to proximity and smartcard readers which provide continuous supervision and monitoring of reader processor and wiring.
integrity by means of a non-proprietary communications protocol standard. Supervision methods that simply supervise wiring or measure current draw are not acceptable, since they do not insure that the reader’s microprocessor is actually operational. Likewise, proprietary protocols which are sole sourced or licensed for a fee are not acceptable, since they limit potential future expansion options for the SMS.

b. The preferred protocol is the Open Supervised Device Protocol (OSDP), since it is non-proprietary and meets the requirements stated above. Alternative supervised reader interface protocols will be considered only if they meet all of the technical requirements of this section AND can be shown to be non-proprietary.

PART 3- EXECUTION

3.1 EXAMINATION

A. Examine substrates, areas, and conditions for compliance with requirements for installation tolerances and other conditions affecting performance of electronic security system.

B. Examine rough-in for embedded and built-in anchors to verify actual locations of intrusion detection connections before electronic security system installation.

C. Proceed with installation only after unsatisfactory conditions have been corrected.

3.2 SYSTEM INTEGRATION

A. Integrate electronic security system with the following systems and equipment:
   Future Systems that may be integrated into the SMS include:
   1. Elevators.
   2. Network lighting controls.
   3. Intercommunications and program systems.
   4. Public address and mass notification systems.
   5. Access control.
   6. Fire-alarm system.
   7. Perimeter security system.
   8. Video surveillance.

3.3 INSTALLATION

A. Install electronic security system in accordance with manufacturer’s written instructions.

B. Wiring Method: Install wiring in metal raceways. Conceal raceway except in unfinished spaces and as indicated. Minimum conduit size shall be 1/2-inch. Control and data transmission wiring shall not share conduit with other building wiring systems. Install wiring in metal 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. 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.

END OF SECTION
### PCC Campus Security Implementation - Door Schedule & Photos

#### Downtown Campus (cont.)
**Levels 1 & 2 - Campus Center & Library, Level 1 Science & Technology**

<table>
<thead>
<tr>
<th>Door No.</th>
<th>Frame / Door Mat.</th>
<th>All Wall Constr.</th>
<th>Middleware</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>STV108</td>
<td>HAMM &amp; GLASS</td>
<td>CMU WALL</td>
<td>N/A</td>
<td>Monitor</td>
</tr>
<tr>
<td>7A-05</td>
<td>HAMM &amp; GLASS</td>
<td>CMU WALL</td>
<td>N/A</td>
<td>Monitor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Northwest Campus
**Buildings A, B - Level 1, Buildings B, D, E - Levels 2 & 3**

<table>
<thead>
<tr>
<th>Door No.</th>
<th>Frame / Door Mat.</th>
<th>All Wall Constr.</th>
<th>Middleware</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2110</td>
<td>HAMM &amp; GLASS</td>
<td>CMU WALL</td>
<td>N/A</td>
<td>Monitor</td>
</tr>
<tr>
<td></td>
<td>HAMM &amp; GLASS</td>
<td>CMU WALL</td>
<td>N/A</td>
<td>Monitor</td>
</tr>
<tr>
<td></td>
<td>HAMM &amp; GLASS</td>
<td>CMU WALL</td>
<td>N/A</td>
<td>Monitor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Door No.</th>
<th>Frame / Door Mat.</th>
<th>All Wall Constr.</th>
<th>Middleware</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Door Schedule & Photos**

<table>
<thead>
<tr>
<th>Door No.</th>
<th>Frame / Door Mat.</th>
<th>All Wall Constr.</th>
<th>Middleware</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
- **Doors are shown to aid the Contractor.**
- **No frame details, schedule of work, etc. are shown in this document.**
- **No indication of the Contractor’s Door Schedule & Photos is shown here.**
- **A door schedule is shown at the end of the Report.**

---

**Contact Information:**

Pima Community College
P.O. Box 20255
Tucson, AZ 85734-8255
Contact: 520-696-2271
Fax: 520-696-2272

**Website:**
PimaCommunityCollege.org

---

**A1.2**
COMMUNITY CAMPUS - LEVEL 2
AREA W - PARTIAL ELECTRICAL PLAN
SCALE 1"=10'

COMMUNITY CAMPUS
LEVEL 1 - OVERALL ELECTRICAL PLAN
SCALE 1"=10'

PimaCommunityCollege
POC SECURITY & DOOR ACCESS
COMMUNITY CAMPUS
LEVEL 1 AREA B
ELECTRICAL PLANS

NOTE: THIS DOCUMENT HAS BEEN PREPARED BASED UPON INFORMATION ACQUIRED ON FIELD OBSERVATIONS AND IS BUILT ONNED. CONSTRUCTION SHALL VISIT THE SITE AND CHECK ALL AREAS prior TO START OF ANY WORK.

E1.1
1. INSTALL NEW CARD READER AT EXISTING INGRESS SYSTEM BOARD WALL.
2. INSTALL NEW CARD READER AT EXISTING EXTERIOR MASTERCARD VENDOR PANEL WALL.
3. PROVIDE 2 1/4" C. TO CEILING SPACE AND MOUNT PIECES ABOVE CEILING TO NEW EXISTING WALL, EQUIPMENT IN EXISTING WET/Dry ROOM.
4. PROVIDE NEW ACCESS CONTROL EQUIPMENT ON WALL AS PER TYPICAL DETAIL E.
5. COORDINATE INSTALLATION WITH EXISTING AUTOMATIC DOOR OPENER INSTALLED AT WINDOW FRAME.
6. PROVIDE 6 POINT ENTRANCE WITH DOOR QUALITY FOR ACCESS CONTROL.
7. PROVIDE PHONE IN A DATA CONNECTION BETWEEN NEW TYPE B ACCESS SYSTEM AND EXISTING COMM. WALL, COORDINATE WITH PCC.
8. PROVIDE ELECTRICAL SYSTEM PER TYPICAL DETAIL #9 THIS SHEET.

SECl/ACCESS CONTROLLER & POWER SUPPLY INSTALLATION DETAIL SCALE: 1/4" = 1'-0"
DISTRICT CORPORATE OFFICE - BUILDING B - LEVEL 2 - ELECTRICAL PLAN

DISTRICT CORPORATE OFFICE - BUILDING E - LEVEL 2 - ELECTRICAL PLAN

DISTRICT CORPORATE OFFICE - BUILDING T - LEVEL 2 - ELECTRICAL PLAN

DISTRICT CORPORATE OFFICE - BUILDING T - LEVEL 2 - ELECTRICAL PLAN

SEC/ACCESS CONTROLLER & POWER SUPPLY INSTALLATION DETAIL

TYPICAL IDF ROOM WALL ELEVATION VIEW

NOTE: THIS DOCUMENT HAS BEEN PREPARED BASED UPON INFORMATION AVAILABLE ON SITE OBSERVATIONS AND AS BUILT DRAWINGS. CONTRACTOR SHALL VERIFY THE SITE AND ENSURE THAT ALL WORK IS ACCORDANCE WITH LOCAL BUILDING CODES AND OTHER DEPARTMENT SPECIFICATIONS PRIOR TO START OF ANY WORK.