TOWN OF SIMSBURY

WATER POLLUTION CONTROL AUTHORITY
36 DRAKE HILL ROAD
SIMSBURY, CONNECTICUT 06070

INVITATION TO BID

DOOR ACCESS SYSTEM REPLACEMENT

Submission Deadline:

Wednesday, September 13, 2017

Submission Contact and Address:

Anthony Piazza
Superintendent
36 Drake Hill Rd
Simsbury, CT 06070
Fax: 860-658-6809
Email: apiazza@simsbury-ct.gov

Purpose:

The Town of Simsbury is soliciting bids for the installation of a door access system at the Water Pollution Control Facility to replace the existing system. Specifications and layout of the WPCA facility can be found in this Invitation to Bid.

TOWN OF SIMSBURY

WATER POLLUTION CONTROL AUTHORITY
36 DRAKE HILL ROAD
SIMSBURY, CONNECTICUT 06070

INVITATION FOR BID

FOR

DOOR ACCESS SYSTEM REPLACEMENT

The Town of Simsbury is soliciting bids for a DOOR ACCESS SYSTEM REPLACEMENT. The scope of work is to include furnishing all labor, materials, equipment necessary for the work as specified.

Sealed bids, endorsed "**Access Control System – Simsbury WPCF**" will be received at the office of the Finance Director, 933 Hopmeadow St., (Route 10/202), Simsbury, Connecticut, until **Wednesday, September 13, 2017 at 11:00 a.m. (EST)** at which time they will be opened in public by the Director of Finance. Bids received after the time set for the opening may be rejected.

Specifications and bidding documents may be obtained electronically via the Town's web site at the following link: http://www.simsbury-ct.gov/finance/pages/public-bids-and-rfp. Bid documents will not be mailed or faxed.

STANDARD INSTRUCTIONS TO BIDDERS
DOOR ACCESS SYSTEM REPLACEMENT
SIMSBURY, CT 06070

1. Project Overview

The Town of Simsbury is soliciting bids for the installation of a new secure door access system to replace the existing. The original door access card reader system (TOPAZ) was manufactured by GE Security. As a result of an acquisition GE Security no longer supports TOPAZ. The system includes (25) Card readers, (40) Door contacts and (14) Glass break detectors. All existing wiring will be re-used along with existing card readers and electric locking devices.

Included in this work is the installation a computer workstation to be used by the door access system that will include a desk computer and monitor, replacement of system lock power supplies with internal Battery backup and related work.

A mandatory Pre-bid Meeting is scheduled for August 23, 2017, at the Simsbury WPCF, located at 36 Drake Hill Road, Simsbury, CT, at 9:00 AM.

Specifications of the proposed door access system can be found in this document in "APPENIX 1 – Door Access System Specifications". A drawing of the facility can be found in "APPENDIX 2 – WPCA Facility Layout".

2. Key Event Dates:

Invitation to Bid Issued	8-11-2017
Mandatory Pre-Bid Conference	8-23-2017
Bids Due	9-13-2017
Commencement of Work	Within ten (10) calendar days of Notice to Proceed

3. Bid Submission Instructions:

a. One (1) original and one (1) copy of all bids must be submitted in a sealed envelope with the bidder's name on the outside of the envelope and clearly marked "**Access Control System – Simsbury WPCF**". If forwarded by mail or courier, the sealed envelope must be addressed to "Sean Kimball, Director of Finance, 933 Hopmeadow Street (Rt. 10/202), Simsbury, CT 06070". Bids must be at the office of the Director of Finance prior to 11 a.m., Wednesday, September 13, 2017. Postmarks are NOT an acceptable waiver of this policy. Once the first bid is opened, all bids are deemed final and no corrections or alterations may be made.

b. Ditto marks or words such as "SAME" must not be used for the bid to be considered.

c. All information must be submitted in ink or typewritten. Errors, alterations or corrections must be shown on both the original and all required copies and each must be initialed by the person signing the bid.

d. Bids are considered valid for ninety (90) days after bids are opened. Bidders may not withdraw, cancel or modify their bid during this ninety (90) day period after bids are opened.

e. An authorized person representing the legal entity of the bidder must sign bids.

f. The inability to meet any specified requirement(s) must be stated in writing and attached to the bid form, or written on the bid form. If no exceptions are noted, it shall be assumed that the terms of the Invitation to Bid have been accepted.

g. The Town of Simsbury reserves the right to waive any minor informality in a bid when such a waiver is in the best interest of the Town.

4. Questions:

Any questions about this project should be directed to: Mr. Anthony Piazza WPCA Superintendent by fax 860-658-6809, email at apiazza@simsbury-ct.gov or by mail Water Pollution Control Authority, 36 Drake Hill Road, Simsbury, CT 06070. To receive consideration, such questions must be received at least five (5) business days before the established date for receipt of bids. No oral interpretations shall be made to any respondent as to the meaning of any of the bid documents. Every request for an interpretation shall be made in writing.

The Town will respond to all appropriate questions received via an addendum available to all prospective bidders. Such addenda will become part of this Invitation to Bid and the resulting contract. At least three (3) days prior to the receipt of bids, the Town will post a copy of any addenda to its website, located at: http://www.simsbury-ct.gov/finance/pages/public-bids-and-rfp. It shall be the responsibility of each bidder to determine whether addenda have been issued, and if so, to download copies directly from the Town's website.

5. Presumption of Bidder Being Fully Informed:

At the time the first bid is opened, each bidder is presumed to have read and is thoroughly familiar with all bidding documents as well as all contract documents for this project. Failure or omission of the bidder to receive or examine any documentation or information concerning this bid shall in no way relieve any bidder from obligations with respect to their bid.

6. Pre-Bid Conference:

A pre-bid conference is scheduled on the project site to allow all prospective contractors to review the project with Town representatives and ask questions. The conference will be located on 36 Drake Hill Road, Simsbury, CT, at 9:00 AM on August 23, 2017. All prospective bidders are encouraged to attend. The Town will provide basic clarifications in response to questions raised, if any material changes to the bid documents or scope of work arise from this conference an addendum will be issued to provide clarity in the bidding process.

7. Interpretation of Acceptable Work:

The specifications, bidding and contract documents are to be interpreted as meaning those acceptable to the Town of Simsbury. The Town will issue any substantive changes or interpretations in writing as an addendum.

8. Tax Exemptions:

The bidder shall be aware that the Town of Simsbury is exempt from Federal Excise Taxes and Connecticut Sales and Use Taxes. Appropriate tax exempt forms will be provided to the successful bidder(s) as part of the contract award process.

9. Insurance Requirements:

The firm must carry insurance under which the Town is named as an additional insured, as follows:

Such insurance must be by insurance companies licensed to write such insurance in Connecticut against the following risks with the following minimum amounts and minimum durations.

A. Workman's Compensation, as required by State Statute & $100,000 employers liability limit.

B. Public Liability, Bodily Injury Liability and Property Damage Liability as follows:

Injury or death of one person:	$2,000,000
Injury to more than one person in a single accident:	$1,000,000
Property damage in one accident:	$1,000,000
Property damage in all accidents:	$2,000,000
Excess/Umbrella Liability:	$1,000,000

C. Automobile and Truck (Vehicular) Public Liability, Bodily Injury Liability and Property Damage Liability as follows:

Injury or death of one person:	$1,000,000
Injury to more than one person in a single accident:	$1,000,000
Property damage in one accident:	$1,000,000
Property damage in all accidents:	$1,000,000

Insurance under B, and C above must provide for a 30 day notice to the Town of cancellation/or restrictive amendment.
Insurance under B and C above must be for the whole duration of the contract and for twelve (12) months after acceptance of the project by the Town.

Subcontractors must carry A, B, and C in the same amounts as above for the duration of the project and until acceptance by the Town.

Certificates of insurance must be submitted to the Director of Public Works prior to the signing of

the contract and within ten days of notification of award of contract. Should any insurance expire or be terminated during the period in which the same is required by this contract, the Director of Public Works shall be notified and such expired or terminated insurance must be replaced with new insurance and a new certificate furnished to the Director of Public Works.

Failure to provide the required insurance and certificates may, at the option of the Town, be held to be a willful and substantial breach of this contract.

10. Substitution for Name Brands:

Should brand name items appear in this bid, the bidder must attach specifications for any substitutions and explain how the substitution compares with the specifications of the named brand. The decision on whether to use the substitution or the named brand rests solely with the Town of Simsbury.

11. Awarding the Bid:

The Town reserves the right to accept any bid or any part of bids, to reject any, all, or any part of bids, and to waive formalities and informalities in the bidding process. The Town at its discretion will award the bid to the lowest responsible bidder. That bidder is the person or firm who is qualified and competent to do the work, whose past performance is satisfactory to the Town and whose bid documents comply with the procedural requirements stated herein.

13. Rejection and/or Cancellation of Bids:

The Town reserves the right to reject or cancel any and all bids, or any part of any or all bids, if such action is deemed to be in the best interest of the Town.

14. Delivery Arrangements: Not applicable

15. Bid Bond: Not applicable

16. Performance Bond: Not applicable

17. W-9 Form

The successful bidder must provide the Town of Simsbury with a completed W-9 Form prior to commencing work.

18. Submittals:

The Bidder shall, as soon as practicable, but not exceed fifteen (15) calendar days, after notification of selection of the award of the bid, furnish to the Owner, in writing the following:

A. Designation of the Work to be performed by the Contractor's own forces
B. Names of the manufacturers, products and suppliers of the principal items of materials proposed for the work
C. Project work schedule

19. Agreement Documents:

The Agreement Documents are defined as:

- The Standard Instructions to Bidders
- The Agreement as executed
- The General Specifications
- The Additional Information for Bidders
- Any Addenda, if issued

END OF STANDARD INSTRUCTIONS TO BIDDERS

ADDITIONAL INFORMATION FOR BIDDERS

1. Each BID must be made on attached Bid Forms and returned intact. BIDDERS will state, both in writing and in figures, the proposed price for each separate item of the work called for in the annexed blank, by which prices will be compared. If any price is omitted, the blank may be filled with the highest price named by any BIDDER for that item or the BID may be rejected. Only one copy of the BID form is required.

2. Any BID may be withdrawn prior to the above scheduled time for the opening of BIDS or authorized postponement thereof. Any BID received after the time and date specified shall not be considered. No BIDDER may withdraw a BID within 30 days after the actual date of the opening thereof. Should there be reasons why the contract cannot be awarded within the specified period, the time may be extended by mutual agreement between the OWNER and the BIDDER.

3. Each BID must be accompanied by a certified check or bank draft, payable to the Town of Simsbury, or a satisfactory BID Bond executed by the bidder and an acceptable surety, in an amount equal to five (5%) percent of the total Base Bid. The certified check, bank draft, or Bid Bond shall be retained as a guarantee that if the proposal is accepted, the Bidder will post with the OWNER, a Performance, Labor and Material Bond in the full amount of the contract, submit the required insurance certificates, and to sign a contract. Attorneys-in-fact who sign Bonds must file with each Bond a certified and effective dated copy of their Power of Attorney.

    a. As soon as the Bid prices have been compared, the OWNER will return the BONDS of all except the three lowest responsible BIDDERS. When the agreement is executed, the bonds of the two remaining unsuccessful BIDDERS will be returned. The BID BOND of the successful BIDDER will be retained until the Performance, Labor, and Material Bond have been submitted and the required insurance certificates have been filed, after which it will be returned. If a BIDDER refuses to sign a contract or cannot obtain satisfactory Bonds, the Owner will retain his Bid security as liquidated damages, but not as a penalty.

    b. The OWNER reserves the right to waive any informality in, or to reject any or all proposals or to accept any proposal which, in their opinion, is in the best interest of the Town of Simsbury whether or not such proposal is the lowest bid. The contractor must be responsible and qualified and have previously done work of a similar nature.

    c. The OWNER may make such investigations as he deems necessary to determine the ability of the BIDDER to perform the WORK, and the BIDDER shall furnish to the OWNER all such information and data for this purpose as the OWNER may request. The OWNER reserves the right to reject any BID if the evidence submitted by, or investigation of, such BIDDER fails to satisfy the OWNER that such BIDDER is properly qualified to carry out the obligations of the Agreement and to complete the WORK contemplated therein.

    d. A conditional qualified Bid will not be accepted.

4. The Contractor to whom the contract shall be awarded must file the requisite Bonds, and certificate of INSURANCE as specified in the General Conditions, and execute said contract in triplicate within ten (10) calendar days from the date when NOTICE OF AWARD is delivered to the BIDDER, and in case of failure to do so, the person or firm will be considered to have abandoned the contract, and the CERTIFIED CHECK or BID BOND shall be forfeited to the Town of Simsbury.

5. BIDDERS must satisfy themselves of the accuracy of the estimated quantities in the BID schedule by examination of the site and a review of the drawings and specifications including ADDENDA. After BIDS have been submitted, the BIDDER shall not assert that there was a misunderstanding concerning the quantities of WORK or of the nature of the WORK to be done. The failure of omission of any BIDDER to do any of the foregoing shall in no way relieve any BIDDER from obligation in respect to his BID.

6. Should a BIDDER find any discrepancy or omission in the Plans or Specifications or is in doubt as to the meaning of any portion of them, he shall notify the Owner, who will then instruct all BIDDERS in writing regarding the points in question.

7. The OWNER, within ten (10) days of receipt of the requisite Bonds, acceptable Insurance Certificates and Agreement signed by the party to whom the Agreement was awarded, shall sign the Agreement and return to such party an executed duplicate of the Agreement. Should the OWNER not execute the Agreement within such period, the BIDDER may by WRITTEN NOTICE, withdraw his signed Agreement. Such notice of withdrawal shall be effective upon receipt of the notices by the OWNER.

8. The NOTICE TO PROCEED shall be issued within ten (10) days of the execution of the Agreement by the OWNER. Should there be reasons why the NOTICE TO PROCEED cannot be issued within such period, the time may be extended by mutual agreement between the OWNER AND CONTRACTOR. If the NOTICE TO PROCEED has not been issued within the ten (10) day period or within the period mutually agreed upon, the CONTRACTOR may terminate the Agreement without further liability on the part of either party.

9. The Contractor to whom this contract shall be awarded will be required to commence work on the ground within ten days from the date of the NOTICE TO PROCEED from the OWNER notifying the Contractor to begin work, exclusive of Final Restoration, and shall complete the work in 60 calendar days. The BIDDER, if he accepts the contract and fails to complete the contract within the allotted time, must pay the sum of $250.00 as liquidated damages for each consecutive calendar day until the completion of the contract.

10. The OWNER will be responsible for payment in accordance with the terms of the Contract. The OWNER reserves the right to retain five percent (5%) of the final contract price for a period not to exceed 12 months from the date of the acceptance of the project.

11. The CONTRACT DOCUMENTS contain the provisions required for the construction of the PROJECT. Information obtained from an officer, agent, or employee of the OWNER or any other person shall not affect the risks or obligations assumed by the CONTRACTOR or relieve him from fulfilling any of the conditions of the Contract.

12. Further, the BIDDER agrees to abide by the requirements under Executive Order No. 11246, as amended, including specifically the provisions of the equal opportunity clause set forth in the

SUPPLEMENTAL GENERAL CONDITIONS.

13. The LOW BIDDER shall supply the names and addresses of major material SUPPLIERS and SUBCONTRACTORS when requested to do so by the OWNER.

14. The BIDDER'S attention is directed to the fact that all applicable Federal and State law, municipal ordinances, and the rules and regulations of all authorities having jurisdiction over construction of the project shall apply to the contract throughout, and they will be deemed to be included in the contract the same as though herein written out in full.

15. No amount shall be included in the BID for Connecticut State Sales Tax or for Federal Excise

BIDDER'S PROPOSAL

Place _____

Date _____

TO: Director of Finance
933 Hopmeadow Street
Simsbury, Connecticut 06070

Sir:

1. Proposal of _____

(hereinafter called BIDDER), organized and existing under the laws of the State of _____

doing business as _____

In compliance with your Invitation to Bid, dated August 11, 2017, Bidder hereby proposes to perform all work for the construction of **ACCESS CONTROL SYSTEM, SIMSBURY WATER POLLUTION CONTROL FACILITY (WPCF)** in strict accordance with the CONTRACT DOCUMENTS, within the time set forth therein, and at the prices shown for each bid item on the Bid Schedule. Any total cost found inconsistent with the unit cost when the bids are examined will be deemed in error and corrected to agree with the unit cost which shall be considered correct.

2. The undersigned BIDDER does hereby declare and stipulate that this proposal is made in good faith, without collusion or connection with any other person or persons bidding for the same work; that no person or persons other than those named herein are interested in this proposal or in the contract proposed to be taken; that no person acting for or employed by the Town of Simsbury is directly interested therein, or in the supplies or works to which it relates, or in any portion of the profits thereof contrary to the ordinances of said Town and laws of the State of Connecticut; that it is made in pursuance of and subject to all the terms and conditions of the Notice and Instructions to Bidders, the Construction Contract, the Detailed Specifications, and the Plans pertaining to the work to be done, all of which have been examined by the undersigned; that the site of the work has been examined; that it is understood that the town, its agents and employees are not to be in any manner held responsible for the accuracy of, or bound by, any estimates, subsurface information or plan of borings relative to the work and appearing on plans or in the foregoing notice; and that all such estimates, etc., are to be considered solely for the purpose of filling out and comparing the several proposals.

* Insert "a corporation", "a partnership", or "an individual" as applicable

3. The undersigned further agrees, in case of a corporation or fictitious trade name, that an acceptable certificate will be filed showing the proper officer or person authorized to sign said contract.

4. And the undersigned agrees to furnish satisfactory bonds and insurance, and to execute within ten (10) days after notice of the award, a formal contract with the Town of Simsbury, for the fulfillment of this proposal, and it is agreed that in case of failure on the part of the undersigned to do so, the certified check or bid bond deposited herewith shall be forfeited to the Town of Simsbury as liquidated damages for such failure.

   Enclosed herewith find Certified Check, or Bid Bond in amount of_____

   _____Dollars ($_____) made payable to the Town of Simsbury as a proposal guarantee which it is understood will be forfeited in the event the Form of Contract is not executed, if awarded to the undersigned.

5. The undersigned BIDDER agrees to abide by the requirements of EXECUTIVE ORDER NO. 11246, as amended.

6. All the various phases of work enumerated in the Detailed Specifications with their individual jobs and overhead, whether specifically mentioned, included by implication or appurtenant thereto, are to be performed by the BIDDER under one of the items listed in the Bid Schedule, irrespective of whether it is named in said list.

7. Payment for work performed will be in accordance with the Bid Schedule, subject to changes as provided for in the Construction Contract. The total of the Bid is for comparison of proposals only. The Unit Prices, as applied to the quantities of work actually completed, will govern for actual payment. The Bidder acknowledges that the unit price will be applied and the final quantities may increase or decrease by up to 25%. If quantities for an item vary by more than 25% pricing may be adjusted by a mutual agreement in the form of a Change Order.

8. It is understood that time is of the essence in this contract and the BIDDER agrees to commence within 10 days after the NOTICE TO PROCEED and complete work within 60 calendar days.

BIDDER_____

Seal, (if a corporation) BY_____

TITLE _____

BUSINESS ADDRESS _____

_____

TELE. (_____) _____

ITEM NO.	ITEMS OF WORK	ESTIMATED QUANTITIES	UNIT PRICES BID WORDS	UNIT PRICES BID FIGURES	AMOUNT **
1	Installation of Access system replacement parts and computer system	Lump Sum			
		TOTAL BID:			

Contractor Signature Date

If a Partnership, the partners are:

Full Name
Residence

_____ _____

_____ _____

_____ _____

If a Corporation, the officers are:

Full Name Residence

_____ President _____

_____ Treasurer _____

_____ Directors _____

_____ _____

_____ _____

(I/We have)
*(I/We have not) previously performed work subject to the President's Executive Order Number 11246 or any preceding Executive Order.

Signed_____

_____

*Cross out words not applicable

NOTE:
Bidder is reminded that in addition to completing and signing the above proposal and bid form, he/she shall also complete and return with the bid:

- Bid Security
- Non-Collusion Affidavit
- Legal Status Form
- Statement of Bidder's Qualifications

TOWN OF SIMSBURY, CONNECTICUT

BIDDER'S LEGAL STATUS DISCLOSURE

Please fully complete the applicable section below, attaching a separate sheet if you need additional space.

For purposes of this disclosure, "permanent place of business" means an office continuously maintained, occupied and used by the bidder's regular employees regularly in attendance to carry on the bidder's business in the bidder's own name. An office maintained, occupied and used by a bidder only for the duration of a contract will not be considered a permanent place of business. An office maintained, occupied and used by a person affiliated with a bidder will not be considered a bidder's permanent place of business.

IF A SOLELY OWNED BUSINESS:

Bidder's Full Legal Name _____

Mailing Address _____

Owner's Full Legal Name _____

Does the bidder have a "permanent place of business" in Connecticut, as defined above?

_____Yes _____No

If yes, please state the full street address (not a post office box) of that "permanent place of business."

_____

IF A CORPORATION:

Bidder's Full Legal Name _____

Mailing Address _____

State in which Legally Organized _____

State Business ID # _____

Current Officers

_____	_____	_____
President	Secretary	Chief Financial Officer

TOWN OF SIMSBURY

BIDDER'S NON-COLLUSION AFFIDAVIT

The undersigned bidder, having fully informed himself/itself regarding the accuracy of the statements made herein, certifies that:

(1) the bid is genuine; it is not a collusive or sham bid;

(2) the bidder developed the bid independently and submitted it without collusion with, and without any agreement, understanding, communication or planned common course of action with, any other person or entity designed to limit independent bidding or competition;

(3) the bidder, its employees and agents have not communicated the contents of the bid to any person not an employee or agent of the bidder and will not communicate the bid to any such person prior to the official opening of the bid; and

(4) no elected or appointed official or other officer or employee of the Town of Simsbury is directly or indirectly interested in the bidder's bid, or in the supplies, materials, equipment, work or labor to which it relates, or in any of the profits thereof.

The undersigned bidder further certifies that this statement is executed for the purpose of inducing the Town of Simsbury to consider its bid and make an award in accordance therewith.

_____ _____

Legal Name of Bidder (signature)
Bidder's Representative, Duly Authorized

_____
Name of Bidder's Authorized Representative

_____
Title of Bidder's Authorized Representative

_____
Date

Subscribed and sworn to before me this_____day of_____, 20___.

_____
Notary Public

STATEMENT OF BIDDER'S QUALIFICATIONS

All questions shall be answered and information given shall be clear and comprehensive. This statement shall be notarized. If additional room is required to answer questions, please attach additional sheet(s) with the supplemental information. The bidder's name shall appear on the top of the supplemental sheets to avoid confusion. The bidder may submit additional information as it deems necessary to enable the Town to judge the bidder's ability to perform the proposed Contract.

A complete statement of Bidders Qualifications shall be submitted for any Subcontractor that will be utilized to satisfy Item 13 of this Statement of Bidders Qualifications.

1. Bidder's full legal name:

2. Permanent main office address:

3. Contact person for this Invitation:

4. Phone and fax numbers and e-mail address of the contact person during normal business hours:

5. Date of organization:

6. Date of incorporation, if applicable:

7. Number of years bidder has been engaged in business under present firm or trade name:

8. Contracts on hand (dollar value, anticipated completion date):

9. General character or type of work performed by the bidder:

10. Has the bidder ever failed to complete any work awarded to it? If so, please explain in detail the circumstances:

11. Has the bidder ever defaulted on a contract? If so, please explain in detail the circumstances:

CONTRACT

THIS AGREEMENT, made this day of 2017,

by and between THE TOWN OF SIMSBURY, Connecticut

hereinafter referred to as the OWNER, and
hereinafter referred to as the CONTRACTOR:

WITNESSETH:

That for and in consideration of the mutual covenants and promises between the parties hereto, it is hereby agreed that:

1. The CONTRACTOR will furnish all of the materials and supplies, equipment, and labor and other services necessary in conformance with these contract documents for the construction and completion of the project described in general as follows:

   ACCESS CONTROL SYSTEM
   SIMSBURY WATER POLLUTION CONTROL FACILITY (WPCF)
   Project No. WPCA 2017-3

2. COMPLETION OF WORK. The Contractor shall commence the work covered by this contract within ten (10) calendar days after the date of receipt of the Notice to Proceed and shall complete the same within 60 calendar days unless the period for completion is extended as provided for in the General Conditions.

3. CONTRACT SUM. The Owner shall pay the Contractor for the performance of said work, subject to additions or deductions provided herein

   dollars ($) in conformity with the bid schedule of prices.

4. The Contract Documents include the following:

   (a) Notice and Instructions to Bidders

   (b) Bidder's Proposal

   (c) Notice of Award

   (d) Contract

   (e) General Conditions

   (f) Supplemental General Conditions

(g) Plans prepared by Simsbury Water Pollution Control Dept. entitled:

Access Control System – Simsbury WPCF

(i) Specifications prepared or issued by
_Simsbury Water Pollution Control Dept. dated July 2017.

5. The OWNER will pay to the CONTRACTOR in the manner and at such times as set forth in the General Conditions and in such amounts as required by the Contract Documents.

6. This Contract shall be binding upon all parties hereto and their respective heirs, executors, administrators, successors, and assigns.

IN WITNESS WHEREOF, the parties hereto have executed, or caused to be executed by their duly authorized officials, this Contract in duplicate, on the date first above written.

OWNER:

Signed, Sealed and Delivered
in the presence of: _Town of Simsbury

BY: _

TYPE NAME: _Lisa L. Heavner

TITLE: _First Selectwoman

CONTRACTOR:

_____

BY: _____

TYPE NAME: _____

TITLE: _____

PROJECT:
DOOR ACCESS SYSTEM REPLACEMENT

Information Needed for Communications on the Project

Name of Company: _____

Location of Company Office: _____

Street: _____

City/State: _____

Zip Code: _____

Mailing Address of Company Office (if different than location):
Street: _____

City/State: _____

Zip Code: _____

Phone No. of Company's Office (include area code) _____

Phone No. of Company's Project Office (if applicable) _____

Company Official Responsible for this Project:_____

Name: _____

Title: _____

Phone No. ( ) _____

Project Supervisor or Foreman: Name____
Phone No. ( ) _____

Person to be contacted in Emergencies after Work Hours:

Name: _____ Phone No. ( ) _____

Person to be contacted in Emergencies on Weekends and Holidays:
Name:_____Phone No. ( ) _____

If any changes to the above information occur during the progress of the work, the Public Works Director shall be immediately notified.

Town of Simsbury
ACCESS CONTROL SYSTEM
SIMSBURY WATER POLLUTION CONTROL FACILITY (WPCF)
Project No. WPCA 2017-3

August 2017

SUPPLEMENTAL CONTRACT SECTION

Chapter 13 of the Code of Ordinances, the Simsbury Code of Ethics, is hereby incorporated by reference as if fully set forth, and is made a part of the Contract Documents. All Contractors shall sign the Acknowledgement Form.

TOWN OF SIMSBURY

Acknowledgement Form and Charter Section 1103 Code of the Town of Simsbury

ACKNOWLEDGEMENT FORM

I have read Section 1103 of the Charter of the Town of Simsbury, the Code of Ethics Ordinance, and the Guidelines issued thereunder. I understand my responsibilities as a Contractor retained by the Town of Simsbury, and I am in compliance with the Charter and the Code of Ethics. I have indicated in the space below any areas of conflict should they arise in matters before our board, commission, agency or department, and I agree to report any future conflicts under the provisions of Section 1103 of the Charter.

Areas of Exception

CONFLICTS OF INTEREST SECTION 1103

CONFLICTS OF INTEREST. It is hereby declared to be the policy of the Town that any elected or appointed officer, any member of any board or commission or any employee of the Town who has a financial interest, direct or indirect, in any contract, transaction or decision of any officer or agent of the Town or any board or commission, shall disclose that interest to the Board of Selectmen, which shall record such disclosure upon the official record of its meetings. Such disclosure of a financial interest, direct or indirect, in any contract, transaction or decision of any officer or agent of the town or of any board or commission shall disqualify such elected or appointed official or such member of a board of commission or such town employee from participation in the awarding, assignment or discussion of said contract, transaction or decision. Violation by any such official, board or commission member or employee of the provisions of this section shall be grounds for his/her removal.

_____
Signature

_____
Name (Please Print)

_____
Date

ACCESS CONTROL SYSTEM
SIMSBURY WATER POLLUTION CONTROL FACILITY (WPCF)

CONTRACTOR'S EXEMPT PURCHASE CERTIFICATE

I hereby certify, under penalties of perjury, that I am engaged in the performance of a construction contract on a project for the following named exempt agency or organization:

Town of Simsbury

Full Name of Agency of Organization

933 Hopmeadow Street
Simsbury, CT. 06070

Address of Same

That such agency is, to the best of my knowledge and belief, exempt from the Sales and Use Tax because it is a

Town

(Town, School, Fire or Police Department, Library etc.,
or other branch of State or Federal Government)

in accordance with Regulation No. 16 of Sales and Use Tax.

That this certificate is issued to cover all purchases of materials and supplies, designated by me, for use of the project referred to above.

Permit No. _ (if any) (signed) _

Contractor

Date: _

Place: _

Firm Name

Address: _

GENERAL CONDITIONS

1. DEFINITIONS

1.1 Wherever used in the CONTRACT DOCUMENTS, The following terms shall have the meanings indicated which shall be applicable to both the singular and plural thereof.

1.2 ADDENDA - Written or Graphic Instruments issued prior to the execution of the Agreement which modify or interpret the Contract Documents, Drawings and Specifications, by additions, deletions, clarifications or corrections.

1.3 BID - The offer or proposal of the BIDDER submitted on the prescribed form setting forth the prices for the WORK to be performed.

1.4 BIDDER -Any person, firm, or corporation submitting a BID for the WORK.

1.5 BONDS - Bid, Performance, and Payment Bonds and other instruments of security, furnished by the CONTRACTOR in accordance with the CONTRACT DOCUMENTS.

1.6 CHANGE ORDER - A written order to the CONTRACTOR authorizing an addition, deletion, or revision in the WORK within the general scope of the CONTRACT TIME.

1.7 CONTRACT DOCUMENTS - The contract including Advertisement for Bids, information for Bidders, BID, Bid Bond, Agreement, Payment Bond, Performance Bond, NOTICE OF AWARD, NOTICE TO PROCEED, CHANGE ORDER, DRAWINGS, SPECIFICATIONS, AND ADDENDA.

1.8 CONTRACT PRICE - The total monies payable to the CONTRACTOR under the terms and conditions of the CONTRACT DOCUMENTS.

1.9 CONTRACT TIME - The number of calendar days stated in the CONTRACT DOCUMENTS for the completion of the WORK.

1.10 CONTRACTOR - The person, firm, or corporation with whom the OWNER has executed the Agreement.

1.11 DRAWINGS - The part of the CONTRACT DOCUMENTS which show the characteristics and scope of the WORK to be performed and which have been prepared or approved by the OWNER.

1.12 ENGINEER - The Town Engineer of the Town of Simsbury, Connecticut, or his designated representative.

1.13 FIELD ORDER - A written order affecting a change in the WORK not involving an adjustment in the CONTRACT PRICE or an extension of the CONTRACT TIME, issued by the OWNER to the CONTRACTOR during construction.

1.14 INSPECTOR - The person appointed by the Town of Simsbury, Conn. to supervise the WORK and shall extend to and include any assistant whom he/she may designate to act in the premises.

1.15 NOTICE OF AWARD - The written notice of the acceptance of the Bid from the OWNER to the successful BIDDER.

1.16 NOTICE TO PROCEED - Written communication issued by the OWNER to the CONTRACTOR authorizing him/her to proceed with the WORK and establishing the date of commencement of the work.

1.17 OWNER - The Town of Simsbury, Connecticut (A Public Body) for whom the WORK is to be performed.

1.18 PROJECT - The undertaking to be performed as provided in the CONTRACT DOCUMENTS.

1.19 SHOP DRAWINGS - All Drawings, Diagrams, Illustrations, Brochures, Schedules, and other data which are prepared by the CONTRACTOR, A SUBCONTRACTOR, manufacturer SUPPLIER or Distributor which illustrate how specific portions of the WORK shall be fabricated or installed.

1.20 SPECIFICATIONS - A part of the CONTRACT DOCUMENTS consisting of written descriptions of a technical nature of materials, equipment, construction systems, standards and workmanship.

1.21 SUBCONTRACTOR - An individual firm or corporation having a direct contract with the CONTRACTOR or with any other SUBCONTRACTOR for the performance of a part of the work at the site.

1.22 SUBSTANTIAL COMPLETION- That date as certified by the OWNER when the construction of the PROJECT or a specified part thereof is sufficiently completed, in accordance with the CONTRACT DOCUMENTS, so that the PROJECT or specified part can be utilized for the purposes for which it is intended.

1.23 SUPPLEMENTAL GENERAL CONDITIONS - Special provisions required by the funding program or Agency (Federal, State, or Local) for participation in the PROJECT and included in the CONTRACT DOCUMENTS. Also such requirements that may be imposed by Applicable State Laws and special characteristics of the PROJECT.

1.24 SUPPLIER - Any person or organization who supplies materials or equipment for the WORK, including that fabricated to a special design, but who does not perform labor at the site.

1.25 WORK - All labor necessary to produce the construction required by the CONTRACT DOCUMENTS, all construction tools, machinery, and equipment, and all materials and equipment incorporated or to be incorporated in the PROJECT.

1.26 WRITTEN NOTICE - Any notice to any party of the Agreement relative to any part of this Agreement in writing and considered delivered and the service thereof completed, when posted by Mail to the said party at his/her last given address or delivered in person to said party or his/her authorized representative on the WORK.

-- PAYMENT --

2. On the first of each month, the Contractor may submit an itemized estimate of work completed up to that time, including an estimate of the portion of lump sum items completed.

He/she must, if requested by the OWNER, submit satisfactory evidence that he/she has paid in full for all labor, materials and equipment included in the monthly estimate. The estimates shall be made on forms furnished by the Town and the Contractor shall certify that the estimate is correct and the work performed is in conformity with the plans and specifications. No later than 31 days after submission by the Contractor, and acceptance by the Town, of the estimate, the Town will pay the estimated cost, less five percent (5%) retained by the Town.

After completion of the project and acceptance by the Town, the Contractor shall submit an itemized final estimate. No later than 31days after acceptance of the final estimate by the Town, the Town shall pay ninety-five (95%) percent of the Contract price. No later than six months after acceptance of the final estimate the Town will pay the five (5%) retained, unless in that time the materials or workmanship in the project shall have been found to be defective.

-- PERMITS DURATION --

3. The Contractor must obtain all necessary permits and pay the fee for them. (Town permits issued at no charge.)

4. Should the Town be prevented or enjoined from proceeding with work either before or after the start of construction by reason of any litigation or other reason beyond the control of the Town, the Contractor shall not be entitled to or assert claim for damage by reason of said delay; but time for completion of the work will be extended to such reasonable time as the Owner may determine will compensate for time lost by such delay with such determination to be set forth in writing.

-- SUPERVISION --

5. The Town will be represented at all times by the WPCA Superintendent or an employee authorized by the WPCA Superintendent to represent him/her; and the WPCA Superintendent or his/her authorized representative shall have sole authority in the interpretation and execution of the contract.

6. The Contractor must have a competent Field Supervisor on the job during all working hours and notify the Town of his/her name and address in writing, and where he/she may be reached normally after working hours. In the event of the absence of the Field Supervisor, the Contractor must appoint a second in command to take responsible charge of the job. The actual performance of work and superintendence shall be performed by the Contractor but the owner shall, at all times, have access to the premises for the purpose of observing or inspecting the work performed by the Contractor.

-- LAYOUT --

7. The Contractor is responsible for all survey related work including, but not limited to, baseline stakeout and offsets. All layout and as-built, if required, work shall be conducted by a surveyor licensed in the State of Connecticut.

-- SITE WORK --

8. The Contractor will be responsible for maintenance of adequate barricades, signs, and warning systems to protect the job and the public.

9. The Contractor shall properly protect all underground and above ground utilities from damage. No interruption shall be caused to any utility without the knowledge of the OWNER.

-- STANDARDS --

10. Whenever a material, article, or piece of equipment is identified on the plans or in the specifications by reference to manufacturers' or vendors' names, trade names, catalogue numbers, etc., it is intended merely to establish a standard and, any material, article, or equipment of other manufacturers and vendors which will perform adequately the duties imposed by the general design will be considered equally acceptable provided the material, article, or equipment so proposed, is, in the opinion of the OWNER, of equal substance and function. It shall not be purchased or installed by the Contractor without written approval.

-- CHANGES IN WORK --

11. The Owner, without invalidating the Contract, may order extra work or make changes by altering, adding to or deducting from the work, the Contract Sum being adjusted accordingly.

-- CORRECTION OF WORK AFTER FINAL PAYMENT --

12. Neither the final Certificate nor payment nor any provision in the Contract Documents shall relieve the contractor of responsibility for faulty materials or workmanship and, unless otherwise specified, he shall remedy any defects due thereto and pay for any damage to other work resulting therefrom, which shall appear within a period of one year from the date of substantial completion.

13. The Owner shall give notice of observed defects with reasonable promptness. All questions arising under this article shall be decided by the OWNER subject to mediation.

14. **INSURANCE REQUIREMENTS**

The Contractor must carry insurance under which the Town as an assured, as follows:

Such insurance must be by insurance companies licensed to write such insurance in Connecticut against the following risks with the following minimum amounts and minimum durations.

A. Workman's Compensation, as required by State Statute.

B. Public Liability, Bodily Injury Liability and Property Damage Liability as follows:

Injury or death of one person:	$1,000,000
Injury to more than one person in a single accident:	1,000,000
Property damage in one accident:	1,000,000
Property damage in all accidents:	1,000,000

C. Automobile and Truck (Vehicular) Public Liability, Bodily Injury Liability, and Property Damage Liability as follows:

Injury or death of one person:	$1,000,000

Injury to more than one person in a single accident:	1,000,000
Property damage in one accident:	1,000,000
Property damage in all accidents:	1,000,000

D. Builders Risk including Fire and Extended coverage:
In an amount equal to the value of construction completed plus materials delivered to the site.

Insurance under B, C, and D above must provide for a 30 day notice to the Town of cancellation/or restrictive amendment.

Insurance under B and C above must be for the whole duration of the contract and for twelve (12) months after acceptance of the project by the Town.

Insurance under D above must be carried for the whole duration of the project and until acceptance by the Town.

Subcontractors must carry A, B and C in the same amounts as above for the duration of the project and until acceptance by the Town.

Certificates of insurance must be submitted to the WPCA Superintendent prior to the signing of the contract and within ten days of notification of award of contract. Should any insurance expire or be terminated during the period in which the same is required by this contract, the WPCA Superintendent shall be notified and such expired or terminated insurance must be replaced with new insurance and a new certificate furnished to the WPCA Superintendent.

Failure to provide the required insurance and certificates may, at the option of the Town, be held to be a willful and substantial breach of this contract.

NOTE: Coverage under "B" shall include XCU coverage as necessary, Collapse and Underground shall be provided for ALL Contracts. Explosion will be provided if specified, or prior to any blasting being performed under the Contract.

15. OWNER'S RIGHT TO DO WORK

If the Contractor fails to prosecute the work properly or fails to perform any provisions of this contract, the Owner, after three days written notice to the Contractor may, without prejudice to any other remedy it may have, make good such deficiencies and may deduct the cost thereof from the payment then or thereafter due the Contractor. Provided, however, that the WPCA Superintendent shall approve both such action and the amount charged to the Contractor.

16. ACCEPTANCE OF FINAL PAYMENT AS RELEASE

The acceptance by the Contractor of final payment shall be and shall operate as a release to the OWNER of all claims and all liability to the CONTRACTOR other than claims in stated amounts as may be specifically excepted by the CONTRACTOR for all things done or furnished in connection with this WORK and for every act and neglect of the OWNER and others relating to or arising out of this WORK. Any payment however, final or otherwise, shall not release the CONTRACTOR or his sureties from any obligations under the CONTRACT DOCUMENTS or the Performance BOND and Payment BONDS.

17. **CONTRACT SECURITY**

The Contractor shall within ten (10) days after the receipt of the NOTICE OF AWARD furnish the OWNER with a performance BOND and a payment BOND in penal sums equal to the amount of the CONTRACT PRICE, conditioned upon the performance by the CONTRACTOR of all undertakings, covenants, terms, conditions, and agreements of the CONTRACT DOCUMENTS, and upon the prompt payment by the CONTRACTOR to all persons supplying labor and materials in the prosecution of the WORK provided by the CONTRACT DOCUMENTS. Such BONDS shall be executed by the CONTRACTOR and shall be in a Form acceptable to the Town Director of Finance. When Surety Company Bonds are used, the corporate bonding company shall be licensed to transact such business in the State of Connecticut and named on the current list of "Surety Companies Acceptable on Federal Bonds" as published in the Treasury Department Circular Number 570. The expense of these BONDS shall be borne by the CONTRACTOR. If at any time a surety on any such bond is declared as bankrupt or loses its right to do business in the State in which the WORK is to be performed or is removed from the list of surety companies accepted on FEDERAL BONDS, CONTRACTOR shall within ten (10) days after notice from the OWNER to do so, substitute an acceptable BOND (or BONDS) in such form and sum as may be satisfactory to the OWNER. The premiums on such BOND shall be paid by the CONTRACTOR. No further payments shall be deemed due nor shall be made until the CONTRACTOR shall have furnished an acceptable BOND to the OWNER.

18. **ASSIGNMENTS**

Neither the CONTRACTOR nor the OWNER shall sell, transfer, assign, or otherwise dispose of the CONTRACT or any portion thereof, or of his/her right title or interest therein, or his obligations there under, without written consent of the other party.

19. **DRAWINGS AND SPECIFICATIONS**

19.1 The intent of the DRAWINGS and SPECIFICATIONS is that the CONTRACTOR shall furnish all labor, materials, tools, equipment, and transportation necessary for the proper execution of the WORK in accordance with the CONTRACT DOCUMENTS and all incidental work necessary to complete the PROJECT in an acceptable manner ready for use, occupancy, or operation by the OWNER.

19.2 In case of conflict between the DRAWINGS AND SPECIFICATIONS, the SPECIFICATIONS shall govern. Figure dimensions on DRAWINGS shall govern over scale dimensions, and detailed DRAWINGS shall govern over general DRAWINGS.

19.3 Any discrepancies found between the DRAWINGS AND SPECIFICATIONS and site conditions or any inconsistencies or ambiguities in the DRAWINGS or SPECIFICATIONS shall be immediately reported to the OWNER, in writing, who shall promptly correct such inconsistencies or ambiguities in writing. WORK done by the CONTRACTOR after his/her discovery of such discrepancies, inconsistencies or ambiguities shall be done at the CONTRACTOR'S risk.

19.4 The OWNER will furnish free of charge to the contractor copies of the DRAWINGS and SPECIFICATIONS as necessary for the proper execution of the WORK.

20. MATERIALS, WORKMANSHIP, SERVICES, AND FACILITIES

20.1 It is understood that except as otherwise specifically stated in the CONTRACT DOCUMENTS, the CONTRACTOR shall provide and pay for all materials, tools, equipment, sanitary conveniences, light, power, transportation, supervision, temporary construction of any nature, and all other services and facilities of any nature whatsoever necessary to execute, complete, and deliver the WORK within the specified time.

20.2 All materials furnished shall be new and of the best quality customarily used in or furnished for work of the character of that herein proposed. Many features of the proposed work are described in detail herein, but the failure to so describe any part of the proposed work or any details or appurtenance thereof shall not be an exception to the above rule. The absence of requirements in drawings or specifications covering details usually included in first class installations of this kind shall not excuse the contractor for their omission in this work.

20.3 All workmanship shall be of the best quality for WORK of the character of that herein proposed. The CONTRACTOR shall employ only competent employees to do the WORK required.

20.4 Materials and equipment shall be so stored as to insure the preservation of their quality and fitness for the WORK. Stored materials and equipment to be incorporated in the WORK shall be located so as to facilitate prompt inspection.

20.5 Materials, supplies, or equipment to be incorporated into the WORK shall not be purchased by the CONTRACTOR or the SUBCONTRACTOR subject to a chattel mortgage or under a conditional sale contract or other agreement by which an interest is retained by the seller.

20.6 Drinking water furnished for the employees on the job shall comply with O.S.H.A. regulations.

21. PROTECTION OF WORK, PROPERTY, AND PENSIONS

21.1 The CONTRACTOR will be responsible for initiating, maintaining, and supervising all safety precautions and programs in connection with the WORK--he/she will take all necessary precautions for the safety of, and will provide the necessary protection to prevent damage, injury or loss to all employees on the site and other persons who may be affected thereby, all the work and all materials or equipment to be incorporated therein, whether in storage on or off the site, and other property at the site or adjacent thereto, including trees, shrubs, lawns, walks, pavements, roadways, structures, and utilities not designated for removal, relocation, or replacement in the course of construction.

21.2 The CONTRACTOR will comply with all applicable laws, ordinances, rules, regulations, and orders of any public body having jurisdiction. He/she will erect and maintain, as required by the conditions and progress of the WORK, all necessary

safeguards for safety and protection. He/she will notify owners of adjacent utilities when prosecution of the work may affect them. The CONTRACTOR will remedy all damage, injury, or loss to any property caused, directly or indirectly, in whole or in part, by the CONTRACTOR, and SUBCONTRACTOR or anyone directly or indirectly employed by any of them or anyone for whose acts any of them be liable, except damage or loss attributable to the fault of the CONTRACT DOCUMENTS or the acts or omissions, of the OWNER or anyone employed by them or anyone for whose acts may be liable, and not attributable, directly or indirectly, in whole or in part, to the fault or negligence of the CONTRACTOR.

21.3 The CONTRACTOR will notify the OWNER at least one week prior to the start of construction.

21.4 The CONTRACTOR shall be responsible for verifying the location of any existing utilities. The CONTRACTOR shall notify "Call Before You Dig" at 1-800-922-4455 such that any utility lines can be marked.

21.5 In emergencies affecting the safety of persons or the work or property at the site or adjacent thereto, the CONTRACTOR, without special instruction or authorization from the OWNER, shall act to prevent threatened damage, injury or loss. He/she will give the OWNER prompt WRITTEN NOTICE of any significant changes in the WORK or deviations from the CONTRACT DOCUMENTS caused thereby, and a CHANGE ORDER shall thereupon be issued covering the changes and deviations involved.

22. CHANGES IN CONTRACT PRICE

The CONTRACT PRICE may be changed only by a CHANGE ORDER. The value of any WORK covered by a CHANGE ORDER or of any claim for increase or decrease in the CONTRACT PRICE shall be determined by one or more of the following methods in the order of precedence listed below:

(a) Unit prices previously approved
(b) An agreed lump sum
(c) The actual cost for labor, direct overhead, materials, supplies, equipment, and other services necessary to complete the work. In addition there shall be added an amount to be agreed upon but not to exceed fifteen (15) percent of the actual cost of the WORK to cover the cost of general overhead and profit.

23. TIME FOR COMPLETION

23.1 The date of beginning and the time for completion of the WORK are essential conditions of the CONTRACT DOCUMENTS and the WORK embraced shall be commenced on a date specified in the NOTICE TO PROCEED.

23.2 The CONTRACTOR will proceed with the work at such rate of progress to insure full completion within the CONTRACT TIME. It is expressly understood and agreed, by and between the CONTRACTOR and the OWNER, that the CONTRACT TIME for the completion of the WORK described herein is a reasonable time, taking into consideration the average climatic and economic conditions and other factors prevailing in the locality of the WORK.

23.3 If the CONTRACTOR is delayed at any time in the progress of the WORK by changes ordered in the WORK, by labor disputes, fire, unusual delay in transportation, unavoidable casualties, causes beyond the CONTRACTOR'S control, or by any cause which the OWNER may determine justifies the delay, then the CONTRACT TIME shall be extended by CHANGE ORDER for such reasonable time as the OWNER may determine.

24. SUSPENSION OF WORK, TERMINATION AND DELAY

24.1 The OWNER may suspend the WORK or any portion thereof for a period of not more than ninety days, or such further time as agreed upon by the CONTRACTOR, by WRITTEN NOTICE to the CONTRACTOR which notice shall fix the date on which work shall be resumed. The CONTRACTOR will resume that WORK on the date so fixed. The CONTRACTOR will be allowed an increase in the CONTRACT PRICE or an extension of the CONTRACT TIME, or both, directly attributable to any suspension.

24.2 If the CONTRACTOR is adjudged as bankrupt or insolvent, or if he/she makes a general assignment for the benefit of his creditors, or if a trustee or receiver is appointed for the CONTRACTOR or for any of his property, or if he/she files a petition to take advantage of any debtor's act, or to reorganize under the bankruptcy or applicable laws, or if he/she repeatedly fails to supply sufficient skilled workmen or suitable materials or equipment, or if he/she repeatedly fails to make prompt payments to SUBCONTRACTORS or for labor, materials, or equipment or if he/she disregards laws, ordinances, rules, regulations or orders of any public body having jurisdiction of the WORK or if he/she disregards the authority of the OWNER, or if he/she otherwise violates any provision of the CONTRACT DOCUMENTS, then the OWNER may, without prejudice to any other right or remedy and after giving the CONTRACTOR and his/her surety a minimum of ten (10) days from delivery of a WRITTEN NOTICE, terminate the services of the CONTRACTOR and take possession of the PROJECT and of all materials, equipment, tools, construction equipment, and machinery thereon owned by the CONTRACTOR and finish the WORK by whatever method he/she may deem expedient. In such case the CONTRACTOR shall not be entitled to receive any further payment until the WORK is finished. If the unpaid balance of the CONTRACT PRICE exceeds the direct and indirect costs of completing the PROJECT, including compensation for additional professional services, such excess SHALL BE PAID TO THE CONTRACTOR. If such costs exceed such unpaid balance, the CONTRACTOR will pay the difference to the OWNER. Such costs incurred by the OWNER will be determined by the WPCA Superintendent and incorporated in a CHANGE ORDER.

24.3 Where the CONTRACTOR'S services have been so terminated by the OWNER, said termination shall not affect any right of the OWNER against the CONTRACTOR then existing or which may thereafter accrue. Any retention or payment of monies by the OWNER due the CONTRACTOR will not release the CONTRACTOR from compliance with the CONTRACT DOCUMENTS.

24.4 After ten (10) days from delivery of a WRITTEN NOTICE to the CONTRACTOR and, the OWNER may, without cause and without prejudice to any other right or remedy, elect to abandon the PROJECT and terminate the contract. In

such case, the CONTRACTOR shall be paid for all WORK executed and any expense sustained plus reasonable profit.

24.5 If, through no act or fault of the CONTRACTOR, the WORK is suspended for a period of more than ninety (90) days by the OWNER or under an order of court or other public authority, or the OWNER fails to act on any request for payment within thirty (30) days after it is submitted, or the OWNER fails to pay the CONTRACTOR substantially the sum approved by the WPCA Superintendent or awarded by arbitrators within (30) days of its approval and presentation, then the Contractor may, after ten (10) days from delivery of a WRITTEN NOTICE to the OWNER, terminate the CONTRACT and recover from the OWNER payment for all WORK executed and all expenses sustained. In addition and in lieu of terminating the CONTRACT, if the WPCA Superintendent has failed to act on a request for payment or if the OWNER has failed to make any payment as aforesaid, the CONTRACTOR may upon Ten (10) Days written notice to the OWNER stop the WORK until he has been paid all amounts then due, in which event and upon resumption of the WORK until he has been paid all amounts then due, in which event and upon resumption of the WORK, CHANGE ORDERS shall be issued for adjusting the CONTRACT PRICE or extending the CONTRACT TIME or both to compensate for the costs and delays attributable to the stoppage of the WORK.

24.6 If the performance of all or any portion of the WORK is suspended, delayed, or interrupted as a result of a failure of the OWNER to act within the time specified in the CONTRACT DOCUMENTS, or if no time is specified, within a reasonable time, an adjustment in the CONTRACT PRICE or an extension of the CONTRACT TIME, or both shall be made by CHANGE ORDER to compensate the CONTRACTOR for the costs and delays necessarily caused by the failure of the OWNER .

25. INDEMNIFICATION

25.1 The CONTRACTOR will indemnify and hold harmless the OWNER and their agents and employees from and against all Claims, Damage, Loss, or Expense including Attorney's fees arising out of or resulting from the performance of the WORK, provided that any such Claims, Damage, Loss or Expense is attributed to Bodily Injury, Sickness, Disease or Death, or to injury to or destruction of tangible property including the loss of use resulting therefrom; and is caused in whole or in part by any negligent or willful act or omission of the CONTRACTOR, and SUBCONTRACTOR, anyone directly or indirectly employed by any of them or anyone for whose acts any of them may be liable.

25.2 In any and all claims against the OWNER, or any of their agents or employees, by any employee of the CONTRACTOR or SUBCONTRACTOR, anyone directly or indirectly employed by any of them, or anyone for whose acts any of them may be liable, the INDEMNIFICATION OBLIGATION shall not be limited in any way by any limitation on the amount or type of damages, compensation or benefits payable by or for the CONTRACTOR or any SUBCONTRACTOR under Workmen's Compensation Acts, Disability Benefit Acts or other Employee Benefits Acts.

25.3 The obligation of the CONTRACTOR under this paragraph shall not extend to the liability of the Owner, his agents or employees arising out of the preparation or

approval of MAPS, DRAWINGS, Opinions, Reports, Surveys, CHANGE ORDERS, Designs, or SPECIFICATIONS.

26. **SEPARATE CONTRACTS**

26.1 The OWNER reserves the right to let other contracts in connection with this PROJECT. The CONTRACTOR shall afford other CONTRACTORS reasonable opportunity for the introduction and storage of their materials and the execution of their WORK, and shall properly connect and coordinate his WORK with theirs. If the proper execution or results of any part of the CONTRACTOR's WORK depends upon the WORK of any other CONTRACTOR, the CONTRACTOR shall inspect and promptly report to the WPCA Superintendent any defects in such WORK that render it unsuitable for such proper execution and results.

26.2 The OWNER may perform additional WORK related to the PROJECT by himself, or he may let other Contracts containing provisions similar to these. The CONTRACTOR will afford the other CONTRACTORS who are Parties to such CONTRACTS (or the OWNER, if he is performing the additional WORK himself), reasonable opportunity for the introduction and storage of materials and equipment and the execution of WORK, and shall properly connect and coordinate his WORK with theirs.

26.3 If the performance of Additional WORK by other CONTRACTORS or the OWNER is not noted in the CONTRACT DOCUMENTS prior to the execution of the CONTRACT, written notice thereof shall be given to the CONTRACTOR prior to starting any such additional WORK. If the CONTRACTOR believes that the performance of such additional WORK by the OWNER or others involves him in additional expense or entitles him to an extension of the CONTRACT TIME, he may make a Claim therefore as provided in Sections 22 and 23.

27. **SUBCONTRACTING**

27.1 The CONTRACTOR may utilize the services of Specialty SUBCONTRACTORS on those parts of the WORK which, under normal contracting practices, are performed by Specialty CONTRACTORS.

27.2 The CONTRACTOR shall not award WORK to SUBCONTRACTOR(s) in excess of Fifty (50) Percent of the CONTRACT PRICE, without prior written approval of the OWNER.

27.3 The CONTRACTOR shall be fully responsible to the OWNER for the Acts and omissions of his SUBCONTRACTORS, and of persons either directly or indirectly employed by him.

27.4 The CONTRACTOR shall cause appropriate provisions to be inserted in all subcontracts relative to the WORK to bind SUBCONTRACTORS, as applicable to the WORK OF SUBCONTRACTORS and to give the CONTRACTOR the same power as regards terminating any subcontract that the OWNER may exercise of the CONTRACTOR under any provision of the CONTRACT DOCUMENTS.

27.5 Nothing contained in this CONTRACT shall create any contractual relation between any SUBCONTRACTOR and the OWNER.

28. **GUARANTY**

The CONTRACTOR shall guarantee all materials and equipment furnished and WORK performed for a period of one (1) year from the date of SUBSTANTIAL COMPLETION. The CONTRACTOR warrants and guarantees for a period of one (1) year from the date of SUBSTANTIAL COMPLETION of the PROJECT that the completed PROJECT is free from all defects due to faulty materials or WORKMANSHIP and the CONTRACTOR shall promptly make such corrections as may be necessary by reason of such defects including the repairs of any damage to other parts of the PROJECT resulting from such defects.

The OWNER will give notice of observed defects with reasonable promptness. In the event that the CONTRACTOR should fail to make such repairs, adjustments, or other WORK that may be made necessary by such defects, the OWNER may do so and charge the CONTRACTOR the cost thereby incurred. The PERFORMANCE BOND or a MAINTENANCE BOND shall remain in force at a value of 25% of the completed WORK through the GUARANTEE PERIOD.

29. **MEDIATION**

29.1 All claims, disputes and other matters in questions arising out of, or relating to, the CONTRACT DOCUMENTS or the breach thereof, except for claims which have been waived by the making and acceptance of Final Payment as provided by Section 16, shall be decided by Mediation in accordance with the Construction Industry Mediation Rules of the American Mediation Association. This agreement to arbitrate shall be specifically enforceable under the prevailing Mediation Law.

29.2 Notice of the Demand for Mediation shall be filed in writing with the Other Party to the CONTRACT DOCUMENTS and with the American Mediation Association, and a copy shall be filed with the Owner. Demand for Mediation shall in no event be made on any claim, dispute, or other matter in question which would be barred by the applicable Statute of Limitations.

29.3 The CONTRACTOR will carry on the WORK and maintain the Progress Schedule during any Mediation proceedings, unless otherwise mutually agreed in writing.

30. **TAXES**

The CONTRACTOR will pay all consumer, use, and other similar taxes required by the Law of the Place where the WORK is performed. This WORK is being performed for a Municipal Government and is exempt from Sales Tax.

SUPPLEMENTAL GENERAL CONDITIONS

1. PA 86-87, AAC Workers' Compensation Insurance Requirements for Contractors on Public Works projects and State licenses, prohibits municipalities from entering into a public works contract with an employer without receiving sufficient evidence from the employer that he has workers' compensation insurance and a statement from the state treasurer that the employer does not owe the Second Injury and Compensation Assurance Fund any money.

2. The Town of Simsbury Water Pollution Control Authority shall be notified at least five (5) days prior to beginning work.

3. A meeting with the WPCA Staff and the Contractor shall be held prior to beginning work. This meeting will be arranged by the WPCA Superintendent.

4. This project involves replacing existing systems. The Contractor shall be responsible for conducting the work such that system service is not interrupted. Any shutdowns may only be permitted by the WPCA Superintendent.

5. Sales and Use Tax Exempt Purchase Certificate/ The Contractor's attention is called to Regulation 18 as amended promulgated by the Sales and Use Tax Division of the State Tax Department, which provided for the Exemption of the sales and use tax on the purchase of such materials and supplies as are to be physically incorporated in and become a permanent part of the project being performed under this contract. The Contractor or Subcontractor shall furnish his suppliers with a completed certificate, in the prescribed form; a copy of which is attached to these specifications

6. Upon completion or termination of the work, the Contractor shall remove from the vicinity of the work all equipment and all temporary structures, waste materials and rubbish resulting from its operations, leaving the premises in a neat and acceptable condition. In the event of failure to do so, the same may be done by the Owner at the expense of the Contractor.

7. The Contractor shall pay for any broken utility lines, except where the utility company may be liable under the "Call Before You Dig" law. The Owner will only pay for relocations necessary to complete the work of this project.

8. In accordance with Executive Order 11246, the Contractor is obliged not to discriminate against any employee or applicant for employment because of race, color, creed, or national origin. This obligation not to discriminate in employment includes, but is not limited to, the following: hiring, placement, upgrading, transfer, demotion, recruitment, advertising, solicitation for employment training during employment, rates of pay or other forms of compensation, selection for training including apprenticeship, layoff, or termination.

SPECIAL PROVISIONS

1. **Cleaning Up**: The Contractor shall at all times keep the site and work free from accumulations of waste material or rubbish caused by his employees or work, or the employees or work of any of his subcontractors.

   On completion of the work, the Contractor except as otherwise expressly directed or permitted in writing, shall tear down and remove all temporary structures built by him; shall remove all rubbish and abandoned materials of all kinds from all Contract structures and from any grounds, streets, or highways which he/she may have occupied; and shall leave all the grounds, streets or highways which may have been affected by his/her operations in a neat and satisfactory condition. Except as noted, all materials salvaged shall be the property of the Contractor.

2. **Weekend Work**: No work shall be done on weekends and holidays.

3. **Contractor To Inspect During Maintenance Period:** Contractor is liable for the maintenance and repair of the system, the Contractor shall inspect the premises and work and ascertain what, if any, repairs are needed, and what incidents occurred which need attention.

   While the town or others may, from time to time, notify the Contractor that such incidents have occurred or that conditions exist needing their attention, such notice by the Owner and others will have been given in the interest of the Town, or other party, and no obligation shall rest upon the Town or agent under this Contract to give such notice. Failure on the part of the Owner or other public officer or other party to notify the Contractor of any incident or circumstances needing repair, or similar service under the maintenance provisions of the Contract shall in no way relieve the Contractor of any part of his duties under the maintenance provisions of the Contract and Specifications.

4. **WPCA Superintendent May Notify Contractor to Make Repairs, Etc**.: The WPCA Superintendent may, from time to time during construction and/or prior to the end of the maintenance period, notify the Contractor that defects exist which should be corrected, drives, walks, etc., are unsafe or inadequately protected by barricades, lights or other means. Upon receipt of such notice from the WPCA Superintendent, the Contractor shall immediately proceed to correct whatever needs attention, if such work is within the obligations of the Contractor under this Contract.

5. **Town May Make Repairs, Etc., at Contractor's Expense**: If, after the Owner has given notice to the Contractor to correct any defects, the Contractor shall fail to do so within a reasonable time thereafter, the Town may cause such defects corrected by such persons or means as it may elect, and the Contractor shall reimburse the Town for any expense incurred by it in performing such work. The Town may deduct from any sum or sums due or to become due to the Contractor such sum or sums as may be proper to reimburse the Town for such expense or expenses, or may collect the costs of such work by other means.

6. **Emergency Repairs, Etc**.: If, in the opinion of the Owner, at any time while the Contractor is responsible for the work or maintenance thereof, an emergency exists where acute danger of damage or injury by reason of inadequate workmanship, protection, or other proper precautions, which it is the duty of the Contractor to provide or to have provided; the Owner may direct the Contractor or the Contractor's representatives to remedy the difficulty immediately; to furnish the urgently needed service.

   If the Contractor or his representative is not present or is not immediately available or able to receive such orders or to perform the emergency services needed, or fails to act following such notice, the WPCA Superintendent, acting for the Town, may, by such persons and means as he deems proper and as are available, take such measures as may reasonably be needed to protect the public, the work, and adjacent persons and property from acute danger of immediate loss, injury, or damage. The Contractor shall reimburse the Town for the expense of any and all such emergency protective measures and the Town may deduct from any sum or sums due to become due the Contractor such sum or sums as may be sufficient to reimburse the Town for its expense for such emergency work.

7. **Act, Or Failure To Act, On Part Of WPCA Superintendent Does Not Reduce Liability Of Contractor**: Giving notice or failure to give notice; or acting as authorized in the preceding sections, or failure to so act, on the part of the WPCA Superintendent; or any question as to the adequacy of the notice by the WPCA Superintendent, or of his/her acts or those of the District, as provided in those sections, shall not in any way relieve the Contractor from any part of his responsibility or liability for performing any and all of the acts and assuming any and all of the risks, duties and liabilities which the Contractor is obligated to perform or assume.

8. **Disposal of Surplus Materials**: The Contractor shall be responsible for the removal and satisfactory disposal of all surplus materials unless otherwise specified in the Detail Specifications. Town properties shall not be used for such disposal unless specifically authorized by the Owner in writing.

9. **Construction Sequence and Restrictions**: In general, the Contractor may determine the direction installation, etc. subject to the approval of the WPCA Superintendent prior to installation. If for any reason whatsoever, however, the WPCA Superintendent shall determine that it is in the best interest of the Town to proceed with the installation in a particular manner or sequence, the Contractor shall do so as directed. Such direction shall not be considered grounds for claim for compensation or damages but shall be considered as having been included in the prices stated in the proposal.

10. **Utility Notification Prior to Excavation**: In accord with Public Act 77-350, the Contractor is required to notify any utility with facilities in the vicinity of the excavation at least two full days prior to excavation. Notification may be given by using the "Call Before You Dig" state wide, toll free telephone number, 811 or 1-800-922-4455., or if the contractor is registered, by e-ticket entry. Responsibility for proper notification of all utilities shall rest with the Contractor.

    a. No claims for extras will be allowed because of any delays, etc. caused by the imposed restrictions; however, additional time may be granted for completion of the work to compensate for any delays caused by said restrictions.

11. **Payment for Appurtenance Installation**: Final payment and retainage release for appurtenance installation will not be made until all inspections are complete.

12. **The State of Connecticut, Tow Building Department and other involved agencies** shall have access and inspection rights to all parts of the work on this project.

13. **Quantities of work** may be increased or decreased by up to 30% with payment to be based on actual quantities of work completed and the bid unit prices.

14. **Submittals or Shop Drawings** shall be submitted to the Owner for review and approval, and shall include all pipe, structures and materials to be utilized to comply with the specifications and drawings. Other samples and certificates of compliance may be requested.

APPENDIX 1
Door Access System Specifications

Door Access System Specifications

PART 1 - GENERAL

1.1 RELATED DOCUMENTS

A. Drawings and general provisions of the Contract, including:

1. Building layout showing doors and gates to be controlled.

2. Location of existing equipment.

1.2 SUMMARY

A. The Security and Database Management System shall be a S2 Security Corporation [NetBox®/NetBoxVR®/Enterprise®] system or approved equal.

B. Section is based on the S2 Security Corporation [NetBox®/NetBoxVR®/Enterprise®] Security and Database Management System (SMS) consisting of computer hardware, software, and associated licensing and equipment for monitoring, recording, and managing Electronic Access Control System (EACS) and Integrated Systems (IS) data and functionality.

C. The Security Management System shall meet the requirements of business and government access control systems. The system shall monitor and control facility access, and shall perform alarm monitoring, camera and video monitoring (when integrated with a compatible future integrated Video Monitoring System), communications loss monitoring, and temperature monitoring. The system shall also maintain a database of system activity, personnel access control information, and system user passwords and user role permissions. The system shall be controlled from a web browser and require no software installation or client licenses. The system shall provide control and access to users on Local Area Networks (LAN), Wide Area Networks (WAN), wireless networks, and the Internet. The system shall provide email and/or text message alerts for all alarm conditions and threats.

D. The SMS includes the following sub-components:

1. Operating Systems (OS) software and firmware

2. Application Software

3. Database Software

4. Network connected Server and Client computer hardware

5. Network connected field level controllers

E. The SMS shall be integrated with monitoring and control systems specified in the following specification sections:

1. Future ability to add in CCTV cameras.

1.3 DEFINITIONS

A. API: Application Programming Interface

B. AVI: Audio Video Interleave

C. CA: Certificate Authority

D. CAC: Common Access Card

E. CE: European Union Conformity

F. CPU: Central Processing Unit

G. CSV: Comma Separated Values

H. DNS: Domain Name Server

I. DSM: Door Status Monitor

J. DVR: Digital Video Recorder

K. EACS: Electronic Access Control System

L. EPS: Events Per Second

M. FCC: Federal Communications Commission

N. FIPS: Federal Information Processing Standard

O. FIFO: First In – First Out

P. FTP: File Transfer Protocol

Q. FRAC: First Responder Authentication Credential

R. GB: Gigabyte

S. GSOC: Global Security Operations Center

T. HA: High Availability

U. HTML: Hypertext Markup Language

V. H.264: Video Compression Standard

W. I^2C: Inter-Integrated Circuit

X. IEEE: Institute of Electrical and Electronics Engineers

Y. I/O: Input/Output

Z. IP: Internet protocol

AA. IS: Integrated System

BB. JPEG: Joint Photographic Experts Group

CC. LAN: Local area network

DD. LDAP: Lightweight Directory Access Protocol

EE. MB: Megabyte

FF. MJPEG: Motion JPEG

GG. MSATA: Mini-Serial Advanced Technology Attachment

HH. MSO: Mobile Security Officer

II. MTBF: Mean-Time Between Failure

JJ. NAS: Network Attached Storage

KK. NBAPI: NetBox Application Programming Interface

LL. NECA: National Electric Code Association

MM. NFPA: National Fire Protection Association

NN. NVR: Network Video Recorder

OO. ODBC: Open Database Connectivity

PP. OS: Operating System

QQ. OVID: Open Video Integration Driver

RR. PDF: Portable Document Format

SS. PIN: Personal Identification Number

TT. PIV: Personal Identity Verification

UU. PoE: Power over Ethernet

VV. PTZ: Pan-tilt-zoom

WW. RAID: Redundant Array of Inexpensive Disks

XX. RAM: Random Access Memory

YY. REX: Request to Exit

ZZ. RFID: Radio Frequency Identification

AAA. RoHS: Restriction of Hazardous Substances

BBB. ROM: Read Only Memory

CCC. RU: Rack Unit

DDD. SFTP: Secure File Transfer Protocol

EEE. SHA: Secure Hash Algorithm

FFF. SIO: Serial Input/Output

GGG. SLA: Sealed Lead-Acid

HHH. SMS: Security Management System or Short Message Service (text messaging)

III. SSL: Secure Sockets Layer

JJJ. SUSP: Software Upgrade and Support Plan

KKK. TCP: Transmission control protocol - connects hosts on the Internet

LLL. TIA: Telecommunications Industry Association

MMM. TWIC: Transportation Worker Identification Credential

NNN. UI: User Interface

OOO. UPS: Uninterruptible power supply

PPP. UTP: Unshielded Twisted Pair

QQQ. VMS: Video Management System

RRR. WAN: Wide area network

SSS. Wi-Fi: Wireless Network

1.4 PERFORMANCE REQUIREMENTS

A. The SMS shall be certified by to meet the following standards:

1. UL294 Listed
2. ISO 9000 Listed
3. CE
4. FCC Part 15
5. RoHS

1.5 ACTION SUBMITTALS

A. Product Data: Provide details and technical specifications for each product indicated. Include physical dimensions, features, performance, electrical characteristics, ratings, software versions, and operating system details.

B. Shop Drawings: Include system line diagrams, equipment locations, installation details, and system integration plans.

1. Detail equipment assemblies and indicate dimensions, weights, loads, required clearances, method of field assembly, components, and location and size of each field connection.

2. Functional Block Diagram: Show single-line interconnections between components for signal transmission and control. Show cable types, quantities, and sizes.

3. Plans and Elevations: Dimensioned plans and elevations of equipment racks, enclosures, and conduit interconnections, including access and workspace requirements.

4. Data Calculations: Provide data bandwidth and storage calculations, including data backup and archive configuration details meeting the minimum project requirements as described herein.

5. Power and Heat Load Calculations: Provide power and heat load calculations for all hardware, including UPS capacity calculations.

6. Wiring Diagrams: For power and signal wiring.

C. Equipment and Software List: Include every piece of equipment and software by product/model name and/or number, manufacturer, serial number, revision number, location, and date of original installation. If factory and/or bench testing regimens are required by the project plan, add pretesting record of each piece of equipment and software, listing name of person testing, date of test, and adjustments made.

1.6 INFORMATIONAL SUBMITTALS

A. UL and ISO9000 Listing Certificates: For SMS components, from manufacturer.

B. Field quality-control reports.

C. Warranty: Sample of product warranty for each system component.

1.7 CLOSEOUT SUBMITTALS

A. Operation and Maintenance Data: For all SMS components and software to include in emergency, operation, and maintenance manuals. In addition to items specified in Section 017823 "Operation and Maintenance Data, include the following:

1. Lists of spare parts and replacement components recommended to be stored at the site for ready access.

2. Operating system, database and application software, including installation, and system configuration backup and recovery data on CD, DVD media or removable storage.

1.8 QUALITY ASSURANCE

A. All work, equipment, materials, construction, and installation provided under the Contract shall comply with the current applicable rules, regulations, standards, and ordinances of the local Authorities Having Jurisdiction (AHJ).

B. Electrical Components, Devices, Accessories, and Installation shall be listed and labeled as defined in NFPA 70, by a qualified testing agency, and marked for intended location and application.

1. Comply with NECA 1.

2. Comply with NFPA 70.

3. Comply with NFPA 101.

C. Software integration between the SMS, VMS, and all other integrated system components shall be tested and certified for interoperability by the manufacturers of each system.

1.9 PROJECT CONDITIONS

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

1. Solid State Network Controller:

a. Operation: Rated for continuous operation in ambient temperatures of 32 to 95 deg F (0 to 35 deg C) and a relative humidity of 5 to 90 percent, noncondensing.

b. Storage: Component storage at ambient temperatures of -4 to 120 deg F (-20 to 49 deg C) and relative humidity of 5 to 90 percent, non-condensing.

2. Network Controller:

a. Operation: Rated for continuous operation in ambient temperatures of 50 to 95 deg F (10 to 35 deg C) and a relative humidity of 5 to 90 percent, noncondensing.

b. Storage: Component storage at ambient temperatures of -40 to 158 deg F (-40 to 70 deg C) and relative humidity of 5 to 90 percent, non-condensing.

1.10 WARRANTY

A. All SMS systems and components shall be provided with an explicit manufacturer warranty of one year for software and two years for hardware. Computer workstation must have a three year warrantee.

PART 2 - PRODUCTS

2.1 OPERATIONAL REQUIREMENTS

A. The Security Management System shall be implemented through network appliance architecture with a three-tiered modular hardware hierarchy and embedded three-tier software architecture.

1. The network appliance shall be capable of running on an existing TCP/IP network and shall be accessible, configurable, and manageable from any network-connected PC with a browser.

2. Browser access for configuration and administration of the system shall be possible from a PC on the same subnet, through routers and gateways from other subnets, and from the Internet. Control and management of the system shall therefore be geographically independent.

3. Security of the data communicated over the network to and from the browser, Network Controller, and nodes shall be protected by encryption (SSL 128-bit) or authentication (SHA-1).

4. The top hardware tier shall be the Network Controller. Embedded on the Network Controller shall be an operating system, a web server, security application software, and the database of personnel and system activity. Converged Video Access systems shall also include fully functional network video recorder.

5. The middle hardware tier shall be the Network Node. The Network Node shall make and manage access control decisions with data provided by the Network Controller, and it shall manage the communication between the Network Controller and Application blades connected to the system's inputs, outputs, and readers. This modular design shall make it possible, even during network downtime, for the system to continue to manage access control and store system activity logs. When network connectivity is re-established, the system activity logs shall be automatically re-integrated.

6. The bottom hardware tier shall be the Application Blades. Four unique Application blades shall be available:

a. Access Control Blade: shall support two readers, four supervised inputs, and four relay outputs.

b. Alarm Input Blade: shall support eight supervised inputs.

c. Relay Output Blade: shall support eight relay outputs.

d. Temperature Blade: shall support eight analog temperature sensor inputs.

B. The SMS shall integrate, within a browser interface, access control, alarm monitoring, video monitoring, and temperature monitoring applications. These applications shall be embedded in a three-tier software architecture.

1. The database tier shall use PostgreSQL. PostgreSQL is a full featured, high performance database management system that supports ODBC. This shall provide a small footprint, low administration, and a high reliability relational database that is embedded without requiring the use of a separate PC server.

2. The web server tier shall be based on an Apache™ embedded web server. This shall provide a graphically rich security management application through a standard web browser.

3. The security application software tier contains the business logic. This application shall also be embedded on the controller and requires no additional memory or processing power.

4. This three tiered embedded software design runs within an embedded Linux Ubuntu operating system and shall require no client-side software other than a web browser.

C. All equipment and materials used shall be standard components, regularly manufactured, and regularly utilized in the manufacturer's system.

D. All systems and components shall have been thoroughly tested and proven in actual use.

2.2 FUNCTIONAL REQUIREMENTS

A. Widget Desktop: The SMS shall provide a widget-based user interface that enables users to create custom monitoring layouts by selecting and arranging widgets on a desktop.

1. Each widget shall provide easy access to a frequently used function—allowing users to, for example, view an activity log, a camera view, or real-time web content.

2. System administrators can save custom layouts for subsequent call up by users, who can then arrange the widgets as desired on their desktops. The administrator shall determine which widgets are available in a layout and the extent to which users can customize the layout. Setup privileges shall enable administrators to switch from "Compose Mode" to "Monitoring Mode" from the desktop menu.

3. When composing layouts, system administrators shall have the ability to display a grid overlay on the Widget Desktop background. Whenever a widget is moved or resized, it will align with (or "snap to") the nearest intersection of lines in the grid. If the grid is saved with the layout, it will appear in the background when users view the layout.

4. The widgets that shall be available for layouts are: Activity Log, Auto-Monitor, Camera View, Clock, Duty Log Entry, Events, Explorer, Floorplans, Intrusion Panel, Passback Grace, PhotoID History, Portal Status, Portal Unlock, Statistics Block, Status, and Threat Level.

5. An Alarm Workflow widget shall be available for layouts. This widget shall allow operators to monitor and resolve alarms within the alarm workflow implemented for the system.

6. When composing layouts, it shall be possible to display vertical and horizontal red lines in the background to assure that positioning widgets within these lines will fit the screen of an iPad or MacBook Air.

B. System Partitioning: The system administrator shall have the ability to divide the SMS into partitions, allowing subsets of the overall population and/or resources to be managed separately.

1. From the default Master partition, one or more additional partitions can be created.

2. Each partition shall contain some number of administrators, card holders with their credentials, and resources.

3. When performing administrative functions, the administrator of a partition shall have the ability to affect only the cardholders and resources in that partition. However, resources can be shared across partitions through the mapping of access levels from one partition to another.

4. System partitioning shall have a precision feature that allows administrators in one or more partitions to view and perform edit functions on person records that belong to another partition.

5. Administrators shall have the ability to search for person records across all partitions to which they have access. The system administrator shall have the ability to make such cross-partition searches the default for users who have access to multiple partitions.

6. After finding a person record located in another partition, an administrator shall be able to click a button to switch to that partition directly from the person record—and possibly edit the record, depending on his or her access rights in that partition. Alternatively, provide the option for making every person record seamlessly visible across all partitions.

C. The SMS shall provide the following Access Control capabilities:

1. Login throttling, which can be enabled for the system to limit the number of login attempts from the same IP address in a given period of time.

2. Integrated photo ID creation capability with video verification.

3. User interface secured access under encrypted password control.

4. System-wide timed anti-passback function.

5. Regional anti-passback with mustering and roll call functions.

6. Region occupancy counting and control.

7. “First-in-unlock” rule enforcement.

8. Multiple access levels and cards per person.

9. 128-bit card support for Wiegand card readers.

10. Detailed time specifications.

11. Simultaneous support for multiple card data formats.

12. Elevator control.

13. Access privileges variable by threat level.

14. Scheduled portal unlock by time and threat level.

15. Card format decoder quickly discovers unknown card formats.

16. Card enrollment by reader or keyboard.

17. Compatibility with various input devices, including biometric readers.

18. Activation/expiration date/time by person with one minute resolution.

19. Access level disable for immediate lockdown.

20. Use of Threat Levels to alter security system behavior globally.

21. Duress PINs, which can be enabled for the system to allow a valid user to raise an alarm if compelled under duress to use his or her credentials (card and PIN) to allow access for another person.

22. Multiple holiday schedules.

23. Timed unlock schedules.

24. Scheduled actions for arming inputs, activating outputs, and locking and unlocking portals.

25. Optional two-man access restriction for portals, requiring two valid card reads from two separate cardholders for portal entry.

26. Card enrollment reader support.

27. Dual-reader portal support.

28. Wiegand Reader support.

29. Magnetic-stripe reader support with cards using ABA Track 2 format for up to 200 bits.

30. Wiegand keypad PIN support for 4-digit or 6-digit PINs.

31. 8-bit and 4-bit burst keypad support for 4-digit or 6-digit PINs.

32. Integration with supported alarm panels.

33. Support for up to 200 DMP intrusion panels with high-level TCP/IP integration.

34. Optional storage and recall of ID photos and personal/emergency data.

35. Unlimited person records.

36. Up to 20,000 credentials are stored locally. An unlimited number of credentials may be authenticated with the controller, caching the most frequently used credentials on the node.

37. Unlimited number of scheduled actions, with the controller downloading up to of 16 per node per day of the soonest-to-activate actions applying to that node, with any others that remain in the database as candidates for downloading later. Expired scheduled actions are removed automatically.

38. The system shall support tracing a person's activity in the current partition if the "Trace this person" check box is selected on the person record.

39. Search for person records using a credential scan.

D. The SMS shall provide the following Monitoring capabilities:

1. The Home page, which is available from the Monitor: Live Monitoring menu on NetBox and NetBox Extreme, lets users view a full system summary, including the Activity Log, Auto-Monitor, and links to frequent User Tasks.

2. Common alarm panel integration for disarm on access, and arm on egress.

3. Support for the direct viewing of IP cameras.

4. Integrated real-time IP-based NVR systems with stored video replay for events.

5. Provides alarms on video loss, video motion detection, and video restore events.

6. Virtual inputs for video fail, camera normal, video motion, and building occupancy limits exceeded.

7. Provides alarms on communication loss and temperature variation.

8. Support for the creation of custom sets of alarm event actions.

9. Provides the ability to record video and link to video for alarm events.

10. Available video control and playback through the S2 SMS user interface.

11. Provides the ability to assign threat levels to various alarms according to severity.

12. Provides the ability to select up to 20 levels of priority for event actions.

13. Provides the ability to enter a duty log comment into the Activity Log, or to append a unique or preset comment to a particular log entry while viewing the Activity Log.

14. Support for the display of Activity Log entries that include both the time the event occurred on the node and the time it was reported to the controller.

15. Support for electronic supervision of alarm inputs.

16. Support for the use of output relays for enabling circuits under alarm event control.

17. A monitoring desktop that integrates video, system activity logs, floorplans, ID photos, and alarm notifications.

18. Support for the creation of unlimited customized monitoring layouts through the use of widgets, including layouts sized for the iPad or MacBook Air.

19. Graphic floorplans with active icons of security system resources.

20. System user permissions to grant whole or partial access to system resources, commands, and personal data.

21. Secure access to the user interface under encrypted password control.

22. Delivery of alerts via browsers, email, and text messages.

23. Remote Logging of system messages to remote host.

E. The SMS shall provide the following Video Management capabilities:

1. Real-time video monitoring displays, including unlimited cameras simultaneously.
2. Playback of event-related video.
3. Video switching and video widget pop-ups based on access activity or event activation.
4. Integrated alarm inputs from the Video Management System (VMS).
5. Digital playback of video events.
6. Linking of video and events based on triggers provided by the S2 SMS or video system.
7. Recall of photo ID and real-time image for comparison.
8. Monitoring and control through a web browser interface.
9. System user permissions to grant whole or partial access to system cameras and video resources.

F. The SMS shall provide the following Security Database capabilities:

1. Maintain data of system activity, personnel access control information, system user passwords and custom user role permissions for whole or partial access to system resources and data.
2. Partitions: It shall be possible to partition the system to create independent, virtual security management systems for multiple populations.
3. Support for the sharing of access levels and user privileges across partitions in a system.
4. Built-in Open Database Connectivity (ODBC) compliant database for personal data.
5. LDAP or SLDAP integration for single-user logon authentication.
6. Unlimited person records.
7. Network-secure API for external application integration.
8. Extensive and easy to use custom report generator.
9. User-defined data fields in personnel records.
10. Record recall by vehicle tag, name, or card.
11. ODBC compliant Database.
12. An API for adding to, deleting from, and modifying the database.
13. Storage of system user passwords and permissions.
14. Storage and recall of ID photos and emergency personal information.
15. Pre-defined reports on system configuration, system activity history, and people.

16. A Used By feature for listing all correlations between specific card readers, keypads, inputs, and outputs, against groups, portals, elevators, access levels, and other configured access control features. This feature may be useful for quickly determining I/O associations when editing and/or deleting system I/O points.

17. An Audit Trail report that shows changes made to the security database over a specified period of time.

    a. For each transaction listed in the report results, information is available on when the transaction occurred, who made the changes, the fields that were modified, and the original and new values.

    b. Search criteria can be applied to filter the report results, either by the person whose record was changed or by the area of the system configuration that was modified.

18. A Credential Audit report that shows all existing access cards by their current status settings. The report also shows for each card the name of the person to whom it was issued and the card number.

19. A Duty Log report shows duty log comments residing in the current security database, including archives.

    a. For each duty log comment included in the report results, information is available on when the comment was entered, who entered it, the date and time of the logged event associated with the comment, the name of the logged event, and the specific comment text.

    b. Search criteria can be applied to filter the report results, either by Operator (the user who entered the duty log comment) or by Event type.

20. English-based query language for instant custom reports.

21. Custom report writer interface that allows the interactive creation of custom reports. Reports may be saved for later reuse. No third party software (such as Crystal Reports) shall be necessary.

22. Custom report scheduling and email distribution.

23. Selectable custom report output formats, including PDF, CSV, and HTML (default).

24. Custom report repository location. Users shall be able to review, cancel and delete reports from this data storage location.

25. Seamless search capability for access history reports. The reporting function shall search the database and archive simultaneously for matching report parameters.

26. Column sorting. Reports output shall be user configurable to sort individual columns in both ascending and descending order.

27. Periodic backup to on-board flash ROM and optional Network Attached Storage (NAS), including FTP and SFTP servers.

28. Periodic archive creation for historical custom reporting and improved on-board database performance.

29. Email and text messaging (SMS) alert notifications.

2.3 HARDWARE REQUIREMENTS

A. The SMS shall employ a modular hardware concept that enables simple system expansion and utilizes a three-tiered hardware hierarchy:

1. At the top tier is the Network Controller, which shall contain the database engine, web server, application software, and configuration data. It is at this level that System Users, through a browser interface, shall interact with the SMS, set configurations, monitor activities, run reports, and manage alarms.

2. At the second tier is the Network Node, an intelligent device with native TCP/IP support, which shall make and manage access control decisions.

3. At the third tier are the application extension blades. Each of these blades shall connect to and manage a set of inputs, outputs, readers, cameras or temperature monitoring points.

4. The network device shall run on existing building TCP/IP networks and shall be configurable for access from separate subnets, through gateways and routers and from the Internet.

5. A MicroNode shall also be available that combines an Access Control blade and a Network Node.

B. The Network Controller shall contain the operating system, database engine, web server, application software, and configuration data. The Network Controller shall be available in four configurations to support small to medium, large, and ultra-large systems.

C. A solid-state NetBox® Network Controller shall contain a processor, flash memory, and a network switch. The Network Controller shall be supplied with 12V DC at a minimum of 5 amps. Internal battery backup shall supply sufficient power to provide for an orderly shutdown of the system in case of loss of external power. External battery backup shall be used to provide uninterrupted operation in the event of external power loss. The Network Controller is accompanied by a Network Node. The Network Node shall contain I^2C for communication with the Application blades and a network interface port. A solid-state Network Controller shall have the following capabilities:

D. The S2 NetBox® Extreme Network Controller shall be available in wall-mount or 2RU rack-mount enclosure. It shall contain a motherboard with an Intel® Atom™ processor and solid-state disk drive. An Ethernet connector shall be provided for network connection. The NetBox Extreme Network Controller shall have the following capabilities:

1.	Nodes/MicroNodes	64
2.	Access control portals	256
3.	Access cards	150,000
4.	Concurrent system users	10
5.	Alarm input points	2000

6.	Control point outputs	2000
7.	Temperature monitor points:	500
8.	Online event history log:	up to 40 Million records
9.	Ethernet ports:	1
10.	Time specifications	512 per partition
11.	Time spec groups	64 per partition
12.	Time specs per group	8 per partition
13.	Threat Levels	8 per partition
14.	Threat Level Groups	32 per partition
15.	Holidays	30 per partition
16.	Access levels per person	32 per partition
17.	Cards per person	100
18.	Report Groups	50
19.	Camera Groups	50
20.	Capacity Rating	10 EPS

E. The Network Node shall make and manage access control decisions with data provided by the Network Controller, and it shall manage the communication between the Controller and Application blades connected to the system's inputs, outputs, and readers. The Node shall be supplied with 120V AC at a minimum of 5 amps. Each Network Node shall support up to seven Application blades except for MicroNodes. Communications between the node and Network Controller shall be encrypted and authenticated (SHA-1). Each Network Node shall have the following capabilities:

1.	Application blades	7
2.	Access control readers	14
3.	Access Levels	512
4.	Portals	14
5.	Portal Groups	64
6.	Readers	14
7.	Reader Groups	128
8.	Supervised Inputs	56
9.	Input Groups	64

10.	Relay Outputs	56
11.	Output Groups	64
12.	Temperature Monitor Inputs	56
13.	Elevators	14
14.	Floors	52
15.	Floor Groups	128
16.	Credential storage	20,000
17.	Activity Log records	27,000

F. The Application blades shall interface with the Network Controller through the Network Node. The Application blades shall be blade-style circuit cards. There shall be four types of Application blades:

1. Access Control blade: shall support 2 readers (input devices such as keypads, RFID devices or Biometric readers), 4 supervised inputs and 4 relay outputs.

2. Supervised Input blade: shall support 8 supervised inputs. Supervised input connectors are 2-pin. The system shall support a wide variety of input supervision types such as: no-resistor, one resistor or two resistor including normally-open circuit and normally-closed circuits.

3. Relay Output blade: shall support 8 relay outputs. Outputs are form C relay represented by 3-pin connectors. Both normally-open circuit and normally-closed circuit output devices are supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.

4. Temperature blade: shall support 8 analog temperature sensor inputs. Temperature range shall be 32° to 158° F (0° to 70° C). Temperature precision within that range shall be ±1.0° F (±0.5° C).

G. The MicroNode® shall combine a Network Node and an Application blade capability in one enclosure. The Access Control blade portion of the MicroNode® shall support two readers, one temperature input, four supervised inputs and four relay outputs. A MicroNode® shall utilize 12VDC power at 3 Amps or Power over Ethernet (PoE) at the 802.3AF standard and be capable of supplying direct power to 2 readers, 2 motion REXs, and 2 door strikes.

2.4 HARDWARE ENCLOSURES AND POWER REQUIREMENTS

A. The Security Management System shall have various hardware enclosures and configurations available to support different installation requirements. Enclosures shall be available for wall or rack mounting. The wall-mount enclosures shall have a lock requiring a key, and a cabinet door tamper switch.

B. The Network Controller supports one solid-state Network Controller blade, a Network Node blade, and seven Application blades. The dimensions are: 17" (431.8 mm) H x 17.5" (444.5 mm) W x 8.25” (210 mm) D.

C. The Network Node Wall-Mount enclosure supports a Network Node blade, and seven Application blades. The dimensions are: 15” (381 mm) H x 17" (431.8 mm) H x 6.75” (171 mm) D.

D. The Rack-Mount Node enclosure supports a Network Node blade, and seven Application blades. The dimensions are: 19" (483 mm) W x 7" (178 mm) H (4U) x 15" (381 mm) D.

E. The Network Controller wall-mount units shall be housed in an enclosure with dimensions of: 12" (304.8 mm) W x 14" (355.6 mm) H x 3.5" (88.9 mm) D. The rack-mount unit dimensions shall be 2U rack x 12" (304.8 mm) D.

F. Network Controllers shall be housed in a 1RU rack-mount enclosure with dimensions of 17.25" (438 mm) W (not including the mounting brackets) x 1.8 " (46 mm) H x 22.4" (569 mm) D.

G. The MicroNode enclosure shall support a solid-state Node, its Access Control blade, and one temperature point.

1. It shall be a wall-mount enclosure with dimensions of 7.2" (183 mm) H x 7" (178 mm) W x 3.58" (91 mm) D.

2. It shall be possible to power the MicroNode with a 12VDC power source at no less than 3 Amps, or from PoE switch that conforms to the IEEE 802.3af standard, which provides nominal 48VDC at a maximum of 400mA.

H. The solid-state Controllers shall be powered by either 100-240V AC at 50-60 Hz, or by 12VDC at 5 amps. Power must come from a separate circuit with an isolated earth ground. If AC power is supplied it must be connected to the internal power supply. If DC power is supplied the internal power supply shall be bypassed. It shall be possible to backup power supplied to the SMS with an Uninterruptible Power Supply (UPS). It shall also be possible to place within the wall-mount enclosure an SLA battery backup sufficient for an orderly shutdown in case of external power loss.

I. Other controllers shall be powered by 100-240V AC at 50-60 Hz. Power must come from a separate circuit with an isolated earth ground and it must be connected to the internal power supply. It shall be possible to backup power supplied to the rack-mounted controllers with an Uninterruptible Power Supply (UPS).

2.5 NETWORK CONTROLLER, NODE, AND APPLICATION BLADE HARDWARE SPECIFICATIONS

A. S2 Solid-state Network Controller - All Application blades shall receive 12VDC power via the ribbon cable bus directly from the Node. The solid-state NetBox Controllers shall be powered by either 100-240V AC at 50-60 Hz, or by 12VDC at 5 amps.

1.	OS	Ubuntu 10.04 LTS
2.	Storage	20GB MSATA(minimum)
3.	Processor	Intel N2800 1.86GHz 2 Cores 4 Threads
4.	RAM	2 GB
5.	Ethernet Ports	1

	6.	Network Nodes Supported	32
	7.	Capacity Rating	5 EPS (events per second)
	8.	Certifications/Compliances	UL, CE, FCC Part 15, RoHS
	9.	Warranty	2 years
	10.	Dimensions (H, W, D)	17in x 17.5in x 8.25in [432mm x 445mm x 210mm]
	11.	Weight	10 lbs. (4.54 kg) (minimum configuration)
	12.	Operation Temperature	0 to 35 degrees C
	13.	Storage Temperature	-20 to +70 degrees C
	14.	Relative Humidity	5-90% non-condensing
	15.	MTBF	105000 hours
	16.	AC Input	85-264 VAC 47-440 Hz 1.5A max @ 115VAC
	17.	BTU Rating	204 BTU
B.	S2 NetBox Extreme Network Controller:		
	1.	OS	Ubuntu 10.04 LTS
	2.	Storage	20GB MSATA(minimum)
	3.	Processor	Intel N2800 1.86 GHz 2 Cores 4 Threads
	4.	RAM	2 GB
	5.	Ethernet Ports	1
	6.	Network Nodes Supported	64
	7.	Capacity Rating	10 EPS (events per second)
	8.	Certifications/Compliances	UL, CE, FCC Part 15, RoHS
	9.	Warranty	2 years
	10.	Dimensions (H, W, D)	14in x 12in x 3.5in [356mm x 305mm x 89mm]
	11.	Weight	7 lbs. (3.18 kg)
	12.	Operation Temperature	0 to 35 degrees C
	13.	Storage Temperature	-20 to +70 degrees C
	14.	Relative Humidity	5-90% non-condensing
	15.	MTBF	105000 hours

16.	AC Input	85-264 VAC 47-440 Hz 1.5A max @ 115VAC
17.	BTU Rating	204 BTU

C. S2 Access Control Blade - The access control blade shall receive power via the ribbon cable bus directly from the Node Blade. The access blade shall supply up to 500 mA of power to one reader or 250 mA of power to each of two readers.

1.	7-pin reader connectors	2
2.	Maximum reader wire length	500 feet (152 m) (18 AWG twisted, shielded)
3.	Power available to readers	500 mA
4.	2-pin supervised input connectors	4
5.	Maximum input wire length	2000 feet (610 m) (22 AWG twisted, shielded)
6.	3-pin relay output connectors	4
7.	Maximum output wire length	Determined by the peripheral device

D. S2 Input Blade - The input blade shall receive power via the ribbon cable bus directly from the Node Blade. It shall support a wide variety of input supervision types including normally-open circuit and normally-closed circuits, and zero, one or two resistor configurations.

1.	2-pin supervised input connectors	8
2.	Maximum input wire length	2000 feet (610 m) (22 AWG twisted, shielded)

E. S2 Output Blade - The output blade shall receive power via the ribbon cable bus directly from the Node Blade. Both normally-open circuit and normally-closed circuit output devices shall be supported. The relay outputs shall support any output devices that operate on the following maximum electrical ratings: 30 Volts DC or AC, 2.5 Amps inductive or 5.0 Amps non-inductive.

1.	3-pin relay output connectors	8
2.	Maximum output wire length	2000 feet (610 m) (22 AWG twisted, shielded)

3. S2 Temperature blade - The temperature blade shall receive power via the ribbon cable bus directly from the Node Blade.

4.	2-pin analog temperature inputs	8
5.	Maximum temperature wire length	1000 feet (305 m) (18 AWG twisted, shielded)

2.6 SOFTWARE REQUIREMENTS

A. Operating System and Application Software:

1. The embedded operating system for the solid-state NetBox®, NetBox Extreme, Exacta50, and Exacta100 Network Controllers is Linux Ubuntu 10.04 LTS (long term support) as the operating platform. The operating system kernel shall be open-source and no operating system training or certification shall be necessary.

2. The SMS application software shall be embedded in the system. The database shall be an embedded PostgreSQL relational database requiring a small footprint and provides high reliability. The web server shall be based on an embedded Apache™ web server enabling users to access and operate the system using a standard web browser.

3. The SMS shall support the following web browsers:

   a. For the SMS (NetBox, NetBox Extreme, and Enterprise) products the listed browsers include; Internet Explorer 11, Internet Explorer 9, Firefox 33, Firefox 32, Safari 6, and Safari 5

B. Software Licensing:

1. Software licensing shall be based upon the number of readers, cameras, and select features for one Network Controller. Software license upgrades shall be available if system reader and camera capacity must be raised. The user license shall be valid in perpetuity and shall include one year of software updates from the date of shipment from the factory.

2. Licensing shall be controlled by a Product Key and an Activation Key. The Product Key contains the licensed system features and limits. To upgrade your system license to enable more cameras or more doors you will need a new Product Key. The Activation Key contains the warranty expiration date. The keys are locked to the system license number. The system license number shall be viewable on-screen on the Support : About page

C. Software upgrades shall be possible from a browser on any network-connected PC, by uploading a software update to the Controller. Controllers shall automatically upgrade all connected nodes. No client software installation shall be necessary.

D. Online Help and Documentation - The SMS shall be provided with complete embedded documentation. The online documentation shall include:

1. Context-sensitive online Help - (The Help displayed is specifically relevant to the current screen.) The online Help system shall provide explanations and procedures for all monitoring, administrative, and system configuration and maintenance functions. The Help system shall have linked table of contents, a linked index, and frequently asked questions pages. Each topic shall also have links to related topics. Each Help topic shall be printable.

2. Technical Support Notes - These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.

3. Installation Guides - These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.

4. Video Integration Guides - These documents shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics.

5. End-User Task Guide - This document shall be in PDF format, shall be printable, and shall be linked to from the Help system table of contents, index, and related topics

E. Support Collaboration - It shall be possible, by the use of a network Support Collaboration Tool, for a technical support specialist to connect to the SMS and assist on-site technicians from remote network-connected locations. It shall only be possible for an on-site system

administrator or technician to initiate this connection. There shall be no way to initiate this connection from outside of the secure network.

F. Language Support - The SMS shall be provided with multiple language support. The ability to switch from one language to another shall be accomplished through the user interface. Translation of the user interface, online help and documentation into other languages shall be available. The languages supported shall include:

1. English
2. Spanish
3. Portuguese
4. French
5. Italian
6. Thai
7. Chinese Traditional
8. Chinese Simplified
9. Japanese

G. Date Formats - The SMS shall support global date formats as follows:

1. mm/dd/yyyy
2. dd/mm/yyyy
3. yyyy/mm/dd

H. Floor plans - The SMS shall provide graphic floorplan capability including graphic display of links to other floorplans, alarms, system resources such as portals, IP video cameras, inputs, outputs, and temperature monitoring points.

1. The Network Administrator holding at least a “Setup” user role shall be able to graphically configure device icons onto the floorplan images, and to upload additional floorplan images. JPEG images shall be supported, and the maximum size for a floorplan image shall be 256K.

2. It shall be possible to create floorplan groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a floorplan group is assigned to a particular system user then the floorplans in that group shall be viewable by that system user.

I. Personnel Data - The SMS shall maintain person data relating to access control, system user privileges, photo identification, system activity, and contact information.

1. All person data in the system shall be integrated onto one tabbed page for viewing, editing, and deletion by system users.

2. A system user holding at least an Administrator user role shall be able to create, delete, and modify person records, including access levels.

3. A system user holding at least a "Setup" user role shall be able to configure the display of person records. For example, the user shall be able to hide various tabs, and configure the User-defined tab by changing the tab label and customizing any of the 20 data fields that appear on the tab. The user shall also be able to define UDF value lists, which can be displayed as pre-entered drop-down lists for user-defined data fields.

J. Data Import and Export - A Data Management Tool shall be provided that supports, via an API, the import and export of personnel data. This tool shall make possible the pre-populating and ongoing populating, of cardholders into the SMS database. Data that shall be importable and exportable shall include:

1. LASTNAME
2. FIRSTNAME
3. MIDDLENAME
4. ACTDATE (activation date)
5. EXPDATE (expiration date)
6. NOTES
7. TEXT1...TEXT20 (user defined fields 1 through 20)
8. ACCESSLEVEL1...ACCESSLEVEL32
9. PERSONID
10. PIN
11. ENCODEDNUM1...ENCODEDNUM10
12. HOTSTAMPNUM1...HOTSTAMPNUM10
13. CARDFORMAT1...CARDFORMAT10
14. BADGELAYOUT
15. JPEG ID PHOTO
16. CONTACT PHONE
17. CONTACT EMAIL
18. CONTACT SMS EMAIL
19. CONTACT LOCATION
20. OTHER CONTACT NAME
21. OTHER CONTACT TELEPHONE

22. OTHER CONTACT TELEPHONE2
23. VEHICLE 1 COLOR
24. VEHICLE 1 MAKE
25. VEHICLE 1 MODEL
26. VEHICLE 1 STATE
27. VEHICLE 1 LICENSE#
28. VEHICLE 1 TAG#
29. VEHICLE 2 COLOR
30. VEHICLE 2 MAKE
31. VEHICLE 2 MODEL
32. VEHICLE 2 STATE
33. VEHICLE 2 LICENSE#
34. VEHICLE 2 TAG#
35. LASTMOD

K. Data Security:

1. Communication between the Network Controller and the browser shall be secured using SSL. In addition, administrative access to the security management application and the personnel data shall be password protected and controlled by roles-based authorizations.

2. Communication between the Network Controller and the Network Nodes shall be encrypted and authentication/tamper detection shall be done using the SHA-1 algorithm.

3. Communication between the Network Controller and other systems (when using the API) shall be secured using SSL and authentication/tamper detection shall be done using the SHA-1 algorithm.

L. Data Backups - It shall be possible to configure regular automatic database backups.

1. It shall be possible to back up a solid-state Network Controller and

2. It shall be possible to back up Controllers to a built-in solid state hard drive.

3. It shall be possible to save backups from any controller to separate network attached storage (NAS), file transfer protocol (FTP) and SFTP servers

4. It shall also be possible to setup regular automatic creation of database archive files.

M. On-board Data Management - Each night the SMS shall truncate a sufficient number of the oldest records held on-board to reduce the database to its set limit, if required. This shall create

the needed storage space for additional system activity records. Truncation will be performed on a First-in, First-out (FIFO) basis.

N. Partitions - It shall be possible to create multiple partitions for the management of multiple security systems or multiple populations.

1. It shall be possible to limit access to the data and resources of one partition to those with permissions for that partition.

2. It shall be possible for each partition to have its own population, resources, rules, events, video management, log data, reports and network resources.

3. It shall be possible to grant Monitor, Administrator and Setup privileges for multiple partitions to the same user. It shall also be possible to create custom user roles for each partition.

4. A node can reside in only one partition. It shall be possible to create partitions without nodes.

O. User Roles and Permissions - There shall be four pre-programmed levels of User Roles, and a total of 16 possible Custom User Roles that can be configured in the system with different permissions for each user:

1. Master Partition Monitor - These users may use the functions in the Monitor menu only within the Master (default) partition. Monitor functions shall include viewing the activity log, cameras, and floorplans.

2. Master Partition Administrator - These users may use the functions of both the Administration and Monitor menus only within the Master (default) partition. Administrative functions shall include adding and editing person information in the enrollment database, issuing and revoking cards, generating reports, and performing database backups.

3. Master Partition Setup - These users may use the functions of the Setup, Administration, and Monitor menus only within the Master (default) partition. Setup functions shall include defining access control, alarm event behavior, camera settings, floorplan images and configurations, holiday and time specifications. Setup functions shall also include: designation of network resources such as time and DNS servers, email and network storage settings; performance of system maintenance such as database backup and restore, software updates and file cleanups; designation of time zone, daily backup schedule and enrollment readers.

4. Full System Setup - These users may use the functions of all menus in all partitions.

5. Custom User Roles - In addition to the roles above the system shall also support the creation of detailed user permissions regarding which data operations, cameras, floorplans, elevators, events, access levels, portals, reports, and personal data fields the system user may see, edit, delete, or control.

P. Alarm Panels - The SMS shall be capable of integrating with alarm panels, arming the panels, disarming the panels, and triggering events based upon alarm panel status.

Q. DMP Intrusion Panels - The SMS shall be capable of integrating with Digital Monitoring Products (DMP) XR500 and XR550 Command Processor Panels.

1. Security administrators can use events on a DMP panel, such as a zone going into an alarm state, to trigger events in the SMS. They can also use events in the SMS to control operations on the DMP panel, such as the arming or disarming of an area.

2. Monitors can use the Intrusion Panel widget to view configuration and status information for a DMP panel. They can also arm and disarm areas, bypass and reset zones, and activate and deactivate outputs associated with the panel.

3. The system shall support at least 200 DMP panels.

4. The DMP panels shall communicate their status to the system using port 6000 (PC Logging)

5. The system shall assign precedence to arm/disarm commands sent from the UI to the DMP panels.

6. DMP system messages shall identify the panel that generated the message.

7. Communication errors between the DMP panels and the S2 SMS shall be re-tried after one minute.

R. Alarm Events - The SMS shall be capable of managing alarm events.

1. It shall be possible to delay an input's change to the Alarm state by a specified number of seconds. The range of delay options shall be 0.5 seconds or from 1 to 120 seconds.

2. It shall be possible to associate specific actions with each alarm event. These actions may include, but are not limited to:

   a. Lock and Unlock portals.

   b. Activate and Deactivate relay outputs.

   c. Arm and Disarm input groups.

   d. Pulse outputs or output groups.

   e. Arm and Disarm alarm panels.

   f. Send emails and SMS messages.

   g. Move cameras to preset positions.

   h. Switch to a video monitor.

   i. Record video.

   j. Momentarily unlock portals.

   k. Change the threat level for a location, and (optionally) for its sub-locations.

   l. Make entries in the activity log.

   m. Play a digital sound file; it shall be possible to specify that it play in a loop until cleared or acknowledged.

n. Display alarms in different colors.

o. Set a priority for an alarm (one of 20 levels, with 1 being the highest).

p. Require a duty log entry.

q. Clear alarm automatically or require an acknowledgement.

3. A system user holding at least a “Setup” user role shall be able to create, delete, and modify alarm system inputs, input groups, outputs, output groups, alarm panels, and events.

4. It shall be possible to trigger events based on system activity such as:

a. Failed login attempts.

b. Video motion detection.

c. Camera failure and camera restore events.

d. Valid or Invalid card reads.

e. Portals held or forced open.

f. Valid card reads with a specified access level.

g. Inputs entering an alarm state.

h. High and low temperature events.

i. Alarm panel arming failures.

j. Alarm panel zone faults.

k. Tailgating and passback violations.

l. Occupancy limit event

m. Zone empty violations.

n. Node power failure, communication failure, timeout, and tamper events.

5. It shall be possible to clone an event which creates an event with all attributes of the original, needing to change only the event’s name and any attributes it will not have in common.

S. Activity Monitoring:

1. The SMS shall support a Monitoring Desktop that integrates video, system activity logs, floorplans, ID photos, and alarm notifications.

2. Activity Log viewing includes one-click navigation to person records.

3. The system shall support a Widget Desktop that allows the creation of custom monitoring layouts. Within a custom layout, widgets display live video, system activity logs, alarm

notifications, ID photos, floorplans, duty log entries, portal status displays, and DMP intrusion panels.

4. The system shall be capable of displaying specific alarm events in the Events and Alarm Workflow widgets in one of the following three modes:

   a. *Activations do not display alarms* – No alarm events shall be displayed in either widget when such events are configured in this mode. All settings shall be disabled in the Acknowledgements section of the page.

   b. *Multiple activations display a single alarm* – Alarm events shall appear in both widgets each time the alarm input is triggered. Each subsequent trigger of the same input shall display a new alarm event which shall replace the previous one.

   c. *Multiple activations display multiple alarms* – Alarm events shall appear in the Events widget as described in item b above. The Alarm Workflow widget shall simultaneously display a separate alarm event for each alarm trigger.

5. Many widgets support multiple partition viewing and filtering. For example, the Activity Log widget can display data from multiple partitions and data filtered by event type or reader group, and/or based on the text content of the event. Additionally, the system shall support the use of category filters, including Access Control, Alarms and Events, Threat Levels, System Admin, Devices, Network Nodes, Access Granted, and Access Denied.

6. It shall also be possible to view cameras, activity logs, and floorplans on separate monitoring pages within the application.

7. The system shall support tracing a person's activity in the current partition if the "Trace this person" check box is selected on the person record. The traced activity is displayed in bold in the color selected for "Trace person log color" on the Network Controller page. In addition, if an event is selected for "Trace person event" on the Network Controller page, it is triggered each time a traced person makes an access attempt. These event activations can be reported using a Trace people filter in a custom history report.

8. The activity log shall be capable of displaying additional cardholder information, including "Hot Stamp", "Encoded Number", and "Company ID".

9. The system shall include a Photo Display Widget, which allows operators to display a current ID photo for based on the most recent access request.

T. Access Control:

1. The SMS shall be able to make access control decisions, define a variety of access levels and time specifications, write system activity into a log file, maintain a personnel enrollment database, receive signals from input devices such as door switch monitors, card readers and motion detectors, energize devices such as door locks and alarms via outputs.

2. Time Specifications: The system shall be capable of storing up to 512 time specifications. Each time specification must be assigned a unique alphanumeric name of up to 64 characters. The definition of a time specification shall require the assignment of both a start time and an end time. Each day of the week shall be individually assignable for inclusion in time specifications. Up to three holiday groups shall be assignable for

inclusion in time specifications. If no holidays are assigned to a time specification then no holiday access shall be allowed.

a. Time specifications shall be assignable to access levels, output groups, portal groups, input groups, and alarm events.

b. Time specifications shall function appropriately per node for the time zone specified for that node.

3. Card Formats -The system shall support the use of readers that use the Wiegand Reader Interface. The system shall support but not require the use of the card facility code. The system shall also support the use of the Magnetic Stripe ABA track 2 card data formats.

a. It shall be possible to create new card formats, designate start bits and bit lengths for facility codes and card ID numbers, as well as designate parity bits. The system shall support up to 32 different card formats. The system shall support card formats up to 128 bits.

b. It shall be possible to reverse the read order of the bits in the facility code and/or card ID portions of a card format.

c. It shall be possible to view and change the default parity bit definitions for a card format.

d. A card formats shall be disabled by default. Once enabled, the format appears in the card format dropdown within the credential section of a person record.

e. The system shall support the use of a concatenated version of the FIPS 201 format (Federal Information Processing Standard Publication 201)

f. FIPS 201 128-bit format. This system-owned credential format is based on Federal Information Processing Standard (FIPS) 201. It can be enabled and disabled, but it cannot be modified. The credential number is a Federal Agency Smart Credential-Number (FASC-N) containing 32 characters, encoded as binary-coded decimal (BCD) digits. When issuing a credential using this format, a user can either enroll the credential via an enrollment reader or use a dialog box to enter a value for each of the fields that make up the 32 BCD string

g. Administrators shall be able to specify a specific number of days of non-use that will be allowed before unused cards will be disabled. Administrators shall be able to exempt individual users from this non-use rule.

h. The system shall support the Southwest Texas Regional Advisory Council (STRAC) UUID format of 128 bits displayed as 32 hexadecimal characters.

4. Access Levels: The system shall be capable of storing unlimited access levels in each partition.

a. Each access level must be assigned a unique alphanumeric name of up to 64 characters.

b. The definition of an access level shall require the assignment of a reader or reader group, and a time specification.

c. It shall be possible to also assign an elevator floor group to an access level.

d. It shall be possible to create a temporary access level by assigning an activation date and/or expiration date for any of a person's assigned access levels. It shall also be possible to have the system automatically remove a temporary access level once it has expired.

5. First-in Unlock Rule: The system shall support the use of a First-in unlock rule. It shall be possible to use this rule to control the unlock behavior of portal groups with assigned unlock time specs.

   a. The First-in unlock rule shall require a card read of a specified access level. The portals in the group shall unlock only when the rule is satisfied and the unlock time spec is valid.

   b. There can be up to 64 First-in unlock rules in the system at a time.

6. Double Card Presentation - The system shall support the use of a Double Card Presentation mode. This mode shall allow the presentation of a card twice in quick succession at a designated reader. Such a "double read" shall change the locked portal to an unlocked state until a subsequent relock event or user-designated timeout occurs. The double card presentation mode shall be enabled on an individual portal basis and shall also require a designation on the access level assigned to the cardholder. The mode shall adhere to time spec and threat level restrictions.

7. Keypad timed unlock - It shall be possible to enable a timed unlock feature for a portal that has a combination reader/keypad device. Once this feature is enabled, any cardholder with valid access to the portal shall be able to specify how long the portal will remain unlocked.

   a. A cardholder presents his or her card and then enters the associated PIN, followed by the number sign (#) and the number of minutes (1-99) the portal should remain unlocked.

   b. The portal will remain unlocked for the specified number of minutes; unless it is closed before the timer expires. If the portal remains open after the timer has expired, a [Door Held Open] alarm will be activated.

   c. If reader/keypad devices are located on both sides of the portal, cardholders will be able to use either device to initiate a timed unlock.

8. Keypad Commands - For Node connected access control keypads and combination card reader/keypads, users having the authorized access levels shall be capable of executing keypad initiated commands based on pre-defined two-digit number codes.

   a. Keypad commands shall be defined by mapping one or more two-digit codes to events defined in the system using the "Setup: Alarms: Keypad Commands" page.

   b. Keypad commands shall be assigned to specific keypads using the "Setup: Access Control: Readers/Keypads" page.

   c. Keypad commands shall be assigned to specific access levels using the "Setup: Access Control: Access Levels" page.

9. Holidays - The system shall be capable of storing up to 30 holidays per partition. Each holiday must be assigned a unique alphanumeric name of up to 64 characters. The definition of a holiday shall require a start date and an end date. Holidays shall have the

ability to span several days using only one holiday slot. Holiday definitions shall support the designation of a start time and an end time. If no start time is designated then the system shall default to 00:00 (start-of-day). If no end time is designated then the system shall default to 24:00 (end-of-day). Holidays shall require the use of 24-hour time format, e.g. 17:00 is 5:00PM.

10. Portals - A portal is any access point and each portal supports up to two readers. The System User, holding at least a "Setup" user role, shall be able to view current portal definitions, change portal definitions, delete portals, and create new portals. Creating a portal defines the access and alarm behavior of the access point. This can include:

    a. Card readers and keypads.

    b. Output for locking.

    c. Input for monitoring the door switch.

    d. Input for a Request-to-Exit function.

    e. Local alarm outputs and system alarm events.

11. Portal Groups - It shall be possible to create groups of portals and to assign an unlock time specification to the entire group. All the portals in the group shall remain unlocked during the time specified.

    a. It shall be possible to use portal groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a portal group is assigned to a particular system user then the portals in that group shall be viewable and unlockable by that system user.

12. Portal Alarm Conditions - Portals shall have four alarm conditions. The four alarm conditions are as follows:

    a. Forced: When a portal is opened and there has been no card read, nor request to exit.

    b. Held: When a portal is held open past the expiration of the shunt timer.

    c. Invalid: When the portal reader reads a card for which there is no entry in the database.

    d. Valid: When the portal reader reads a card for which there is a valid entry in the database.

13. Two-man entry restriction: It shall be possible to require two valid card reads by different cardholders within a specified number of seconds for entry to a specific portal.

14. Escort Rule - The system shall be capable of supporting escorted access control rules by assigning one of the following two escort types to each cardholder:

    a. Escort - Cardholders with this access level shall enable access for persons requiring escorted access by presenting their credential at a card reader within 15 seconds after those requiring escorted access.

b. Requires Escort - Cardholders with this access level shall be unable to access the portal unless a valid “Escort” cardholder presents their credential at the card reader within fifteen seconds after the “Requires Escort” credential has been presented. Otherwise, access will be denied and the Activity Log shall display a message with the reason code {NO ESCORT}.

15. The system shall support Facility Code Mode with the following available options.

a. None (the default): The facility code is treated as part of the overall encoded credential number. A card matching only the facility code will not be granted access.

b. Configuration: Facility-code only checking is turned on only while the complete set of credentials is being downloaded to the Mercury panel. Once the credential download is complete, the behavior is the same as for the “None” setting.

c. Offline: Facility-code only checking is turned on only when the SIO is disconnected from its Mercury panel (via the RS-485 link). When the SIO is connected to the panel, the behavior is the same as for the “None” setting.

d. Configuration and Offline: Facility-code only checking is turned on both during the credential download and when the SIO is disconnected from its Mercury panel. At all other times, the behavior is the same as for the “None” setting.

e. Permanent: Facility-code only checking is turned on at all times.

16. Anti-passback - The system shall support both regional and timed anti-passback access control. For anti-passback functions, it shall be possible to configure regions, assign readers to those regions, and specify events for response to tailgate, passback, and occupancy limit violations. It shall also be possible to designate parent regions for hierarchical anti-passback.

a. Grace: It shall be possible for a system Monitor or Administrator to Grace Card holders from passback and tailgate violations.

b. It shall also be possible to set a specific time for all cardholders to be graced daily.

c. The system shall be able to automatically place the cardholder in a predefined region upon the selection of the grace option.

17. Mustering - To aid in evacuation management it shall be possible to designate a region or regions for mustering. It shall be possible to quickly get an occupancy count and occupant list for any region.

18. Scheduled Actions - It shall be possible to specify system actions to occur at scheduled times. When scheduling an action, it shall be possible to specify whether the time specifications for the scheduled action will be based on the time zone set for the local Network Node or the time zone set for the Network Controller. Scheduled actions can include:

a. Arming and disarming inputs.

b. Activating and deactivating outputs.

c. Locking and unlocking portals.

19. Floor plans - The system shall be capable of displaying active graphic floorplans and configuring each floorplan with icons representing system resources: cameras, portals, temperature points, and alarms. A network administrator holding at least a “Setup” user role shall be able to upload floorplan images and graphically configure device icons onto the floorplan images. Viewing floorplans will require the Macromedia Flash Player 9.0 plug-in for the browser.

    a. It shall be possible to create floorplan groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If a floorplan group is assigned to a particular system user then the floorplans in that group shall be viewable by that system user.

20. Elevator Control - The system shall be capable of controlling elevator access to floors. The system shall be capable of controlling up to 52 floor buttons per node. It shall be possible to create, change, or delete floor groups to assign a free access time specification to a floor group. The floors in this group will be freely accessible during the times defined by the chosen time specification.

    a. It shall be possible to create elevator groups for the purpose of assigning or withholding assignment of these groups to system user permissions known as Custom User Roles. If an elevator group is assigned to a particular system user then the elevators in that group shall be viewable by that system user.

    b. Users assigned to custom user roles for one or more elevator groups may be given Free Access privileges to manage access to the elevators in those groups by using the Scheduled Actions page or an Elevator Status widget to:

        1) Momentarily enable free access for an elevator floor button. This will allow persons to temporarily access one or more floors without the need for an access control transaction such as a card read.
        2) Schedule an extended period of free access to one or more floors. This will allow persons to access the floors without constraints for the duration of the free access schedule.

    c. Floor Tracking - Users may configure optional inputs on the SMS that shall change state when a corresponding floor selection button on an elevator is pushed, enabling the system to monitor the status of each floor selection button in relation to specific access credential transactions.

    d. The system shall support Elevator Floor Tracking

        1) The system shall support optional inputs that change state when the corresponding floor-select buttons are pushed, allowing the system to detect each button’s status.
        2) The system shall support an optional input that will change state and trigger an event, when the elevator’s duress/emergency button is pushed.

    e. Users may configure an optional input for each elevator, and corresponding event on the SMS when the elevator’s duress/emergency button is pressed.

U. Threat Levels:

1. It shall be possible to configure up to eight threat levels. It shall be possible to alter security system behavior through the use of threat levels. Groups of threat levels may be created and assigned to portal groups, access levels, input groups, output groups, floor

groups, and event actions. The behavior of groups, access levels, and event actions with assigned threat level groups shall change based upon the current system threat level.

2. The SMS shall support 32 threat level groups.

3. It shall also be possible to change the system threat level in response to an alarm event.

4. The current system threat level shall display in the title bar of the security application interface and on floorplans.

V. Location-based threat levels - The system administrator shall have the ability to define locations. This allows for threat levels to be assigned to individual locations.

1. Within each parent location, sub-locations can be created, and additional sub-locations can be created within each of these, and so on. This creates a location hierarchy.

2. Portals can be assigned, and threat levels applied, to any location within the hierarchy.

W. Appropriate Use banner - The system administrator shall have the ability to enter text (such as an appropriate use statement) to be displayed on the login page.

X. Reports:

1. The SMS shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system. In addition, an easy to use query language shall be included to create ad hoc reports. The query language shall be documented in the online help system. Alternatively, it shall be possible to specify a query by use of point-and-click.

2. It shall also be possible to produce reports directly from the Network Controller based on data in archive files on FTP or SFTP servers, network attached storage, or the built-in hard drive.

3. The SMS shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a PDF file or put into a spreadsheet.

4. It shall also be possible to group reports for assignment to custom user roles. Any reports not grouped and assigned to a custom user role shall not be viewable by that system user.

5. The system shall be capable of sorting users by various criteria, including email address, and allow for email groups to be selected for auto-distribution.

6. Report generation shall not affect the real-time operation of the system.

7. The specific reports provided shall include the following:

a. Configuration Reports

1) As Built - A graphical report that displays an image of each Application blade in a node and the specific resources (inputs, outputs, readers, etc.) configured for that blade. The network settings for the node shall also be included.

2) Cameras - Displays all camera configuration information including control address, IP port, and camera type.
3) Camera Presets - Displays configured presets for each camera in the system.
4) Elevators - Displays elevator configuration information including node, reader, floor to output mappings, floor select and duress/emergency inputs.
5) Floor Groups - Displays all configured floor groups for use in elevator control.
6) Holidays -Displays holiday specification information.
7) Portals - Displays portal definition information including reader, DSM input, REX input, alarm outputs, and events.
8) Portal Groups - Displays a list of all defined portal groups.
9) Reader Groups - Displays defined groups of readers.
10) Remote Locksets - Available if the Remote Locksets feature is licensed for the system. Displays the following information for each remote lockset: name, IP address, synchronization status, serial number, last completed update time, firmware version, battery voltage, assigned remote lockset profile, and number of stored cardholders. The report can be sorted by any of the columns.
11) Resources - Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.
12) Threat Level Groups - Displays all configured threat level groups and the threat levels assigned to them.
13) Threat Levels - Displays all configured threat levels including the description and color assignment.

b. History Reports

1) Access History - Displays access history based on an entered query. The system user can specify the query using either the keyboard or point-and-click selection. Access history reports shall include the ability to include elevator access requests.
2) Custom Report - This provides the capability to create custom reports of historical data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Custom report output shall be user selectable for HTML, PDF or CSV format. Custom report configuration shall include page size, orientation, column width and shall automatically notify the user if the selected configuration exceeds the selected page size.
3) General Event History - Displays time, type of activity, and activity details for a variety of event types. The system user can select the specific event types for the report.
4) Portal Access Count - Display how many times users have used a portal.
5) Audit Trail - Displays an audit trail of system changes and the name of the system user that made the changes. It shall be possible to specify the dates and times covered in the report.
6) Duty Log - Displays duty log comments residing in the current security database, including archives. For each duty log comment, the report shows the date and time the comment was entered, the person who entered the comment, the date and time of the logged event associated with the comment, and the Activity Log message followed by the specific comment text.

c. People Reports

1) Access Levels - Displays all access levels entered into the system including time specification, reader/reader group, and floor group.
2) Credential Audit - Lists existing credentials by their current status settings (such as Active, Damaged, Lost, or Not Used). Before running the report, users can filter the data to see only credentials with a particular status setting, or only credentials that were not used with a specific number of days from the date they were issued.
3) Current Users - Displays a list of all security system users currently logged in to the security system website.
4) Custom Report - This provides the capability to create custom reports of personnel data. A graphic interface provides the user with the ability to interactively create and save reports for later use. Parameters can be inserted into reports to prompt for data input at report runtime. Custom report output shall be user selectable for HTML, PDF or CSV format. Custom report configuration shall include page size, orientation, column width, and shall automatically notify the user if the selected configuration exceeds the selected page size.
5) Occupancy - Displays a list of defined regions with the number of people currently occupying each region and the maximum number of occupants allowed, if a maximum has been specified.
6) Photo ID Gallery - Displays all the photo ID pictures in the system and the person's name.
7) Photo ID Requests -Displays all outstanding badge print requests and lists ID, name, badge layout, activation date, request date.
8) Portal Access - Lists people with access for a selected portal.
9) Roll Call - Allows you to select a defined Region from the drop-down and see a list of people currently in that region.
10) Roster - Displays every person entered into the system and it lists name, ID photo, expiration date, username, and access level.
11) Time Specifications - Displays all defined time specifications currently in the system.

Y. Administration - The SMS shall provide for the performance of system administration tasks from any network-connected computer with a browser. Most of the administrative, maintenance, and configuration utilities and functions shall require a SMS user with at least a “Setup” user role. Information from the network administrator shall, in many cases, also be required. These administrative tasks shall include but not be limited to:

1. Generating reports:

a. The system shall be capable of producing a variety of predefined reports regarding software and security hardware configuration, event history, and the administration of people within the system.

b. Alternatively, the system shall support a graphic interface for interactively building custom reports from either historical or personnel data. These reports shall be savable for later reuse. Parameters can be inserted into reports to prompt for data input at report runtime. Report results can be printed, output to a pdf file or put into a spreadsheet.

c. It shall also be possible to group reports for assignment to custom user roles. Any reports not grouped and assigned to a custom user role shall not be viewable by that system user.

d. A system user holding “Administrator” permissions shall be able to view and create reports.

2. Database backups:

    a. The system shall create database, or full system data backups, each night at 00:15 hours. These backups shall be stored in ROM and written to the drive on the disk-based controller.

    b. Backups shall also be written to network attached storage (NAS), an FTP server, or an SFTP server if such storage has been configured in the system.

    c. It shall also be possible for the system users to create such database backups at any time. Any database backups onboard the Network Controller may also be downloaded to off controller storage by the system user at any time.

3. System restore:

    a. The system shall be able to restore its database, or the full system data, from a backup. Restoration of the system shall only be possible from a backup copy onboard the Network Controller. It shall, therefore, be possible to upload a copy of a database backup from any network attached storage.

    b. It shall be possible to review backups by date and description and select the desired backup for upload to the Network Controller or restoration as the current system database.

4. Software updates:

    a. Software updates, upgrades and patches shall be provided from time to time. The system shall be able to update its software from these .upg files. Update of the application software shall only be possible from an update file onboard the Network Controller. It shall, therefore, be possible to upload a copy of the software update from any network attached storage or from any PC drive or desktop.

    b. Software updates may involve the Network Controller only or may include updates for the node(s) also. The monitoring of the security system may be unavailable for several minutes during this process.

5. File upload - The system shall support uploads of files for use in and with the system. Files which shall be uploadable include:

    a. Floorplans in jpg format

    b. Badge layouts

    c. ID photos in jpg format

    d. Database backups

    e. Software license files

    f. software updates

    g. Threat level icons in jpg format

    h. Sound files (.wav) for use in event alerts

6. Setting system time, time zones, and time servers:

    a. The SMS shall support the setting of time zones by selection off of a drop down pick list. Time zones shall be separately settable for the controller and for each node or MicroNode in the system. An extensive list of world-wide time zones shall be provided. Adjustments for daylight saving time (summer time) shall be automatic.

    b. The SMS shall support the use of network time servers. Up to three time servers can be designated. Use of a network time server ensures that the Network Controller and its nodes will be regularly synchronized with the exact time used by all other network resources.

    c. It shall also be possible to manually set the system date and time.

7. Changing passwords:

    a. Person data maintained in the system may also contain a user name and password for logging on to the security application website as a system user. The system shall support the changing of administrator passwords. It shall be required to enter the password twice for verification purposes.

    b. Administrators shall be able to specify a minimum number of characters that users must include in their login passwords.

    c. Administrators shall be able to specify that users' login passwords must contain a combination of letters, numbers, and special characters.

    d. Administrators shall be able to set a password expiration period in months (from 1 month to 12 months) for all passwords in the current partition. Whenever a user changes his or her password, it will remain in effect for the selected number of months.

    e. It shall also be possible to integrate an LDAP or SLDAP server for single-user logon authentication. This will reference the LDAP-stored password for use by the system.

8. Issuing and revoking cards (credentials):

    a. Access cards shall be assignable by the system user either by entering card data directly into the person record or by use of an enrollment reader. Access levels shall be assignable through the user interface by selection from the list.

    b. Access cards shall be revocable at any time. A system user holding at least the Administrator user role may perform this action. Revoked cards shall stop functioning immediately.

    c. A system user holding at least the Administrator role may also disable an access card by changing its Active status to Clear, Damaged, Disabled, Expired, Forgotten, Lost, Missing Active, Missing Disabled, Not Returned, Not Used Not Validated, Returned, Stolen, Suspended or Temporary Expired. The card will not function with any of these status settings (unless the setting has been customized, as described below). Running a Credential Audit report shall allow existing cards to be viewed by their current status settings.

d. A system user holding at least the Administrator role may customize any of the following access card status settings: Clear, Damaged, Forgotten, Lost, Not Returned, Not Validated, Returned, Stolen or Suspended. The user can change the name and/or description of the status setting, and can specify that a card to which the setting is applied will continue to function.

e. A maximum number of active cards per person can be enabled for the system. Once a person has reached the system limit, a new card can be added for that person only if one of his or her active cards is revoked or disabled.

f. When “Enable credential profiles” is selected on the Network Controller page, it shall be possible to assign credential profiles to individual credentials to determine the number of days of non-use before they expire.

g. It shall be possible to set expiration dates for individual credentials in a person record. When a controller encounters an expired person record during its nightly system check, it shall modify that person record from “Active” to “Expired”. Similarly, if an expired person record is set to “Temporary”, it shall be changed to “Temporary Expired”.

1) In order to reactivate “Expired” and “Temporary Expired” credentials, a system user with appropriate user role permissions may edit the person record in the User Interface, and modify the expiration date to a future date/time. Once the record is saved, the person record status will be changed to “Active” or “Temporary”.

h. It shall be possible to specify that any credential not used within a specific number of days from the date it was issued will be disabled automatically.

i. The “First Name”, “”Middle Initial”, and “Last Name” fields of each Person Record shall allow for up to 50 characters each.

j. The system shall provide for a workflow to be configured to facilitate processing of lost and/or forgotten credentials.

k. The system shall track credential status information and make it available for use in creating up-to-the-minute credential status reports.

9. Enrolling new people:

a. All person data entered into the system shall be held in the system database and shall be available only to system users holding at least the Administrator user role.

b. Person data can be added, deleted, and edited by users holding at least the Administrator user role.

c. The system shall support person record templates.

1) Each template defines values for specific fields, such as a default set of access levels.
2) These values will be filled in automatically in any person record created from the template.
3) When adding a person to the system, a user shall be able to use one of the available templates in the active partition to create the person record, or create it without a template.

4) Person Record Templates shall be available for use in custom People report definitions and in person search criteria.

10. Creating Photo IDs - The system shall include an integrated photo ID function. It shall be possible:

a. To design badge layouts.

b. To upload badge layouts for badge printing.

c. To capture ID photo images, print badges, and delete uploaded badge layouts.

d. For the system user to manage all photos ID functions entirely from within the browser.

e. To track the number of times a badge has been printed.

f. To print multiple badges at once using the Badge Print Workflow.

g. To enroll a person's card number manually or through a reader and save the new credential from the Badge Print Workflow.

h. The system shall be capable of automatically generating auto-incremental encoded credential numbers. Each new encoded credential number shall be increased by one over the next highest number in the system.

11. Configuring network resources:

a. DNS - The system shall support setting IP addresses for up to two domain name servers.

b. Email settings - The system shall support the use of email notifications of alarm events. The system user must setup the email server IP address or DNS name and the email address of the Network Controller. A network administrator must setup the network mail server to relay email for the IP address of the Network Controller.

1) When setting up an email relay, users shall be able to select a port number other than 25 to indicate that the system should attempt to use encrypted SSL connections for the outgoing messages. If an encrypted connection is not available, then the system will fall back to port 25 for an unencrypted connection.

c. File transfer protocol (FTP) - The system shall support the use of an FTP or SFTP Server for backups. Once configured, backups are automatically saved to the FTP server each night.

d. NAS - The system shall support the use of network attached storage devices for backups. The network administrator must create a domain user account for the Network Controller and a password. The system user must configure the network attached storage in the system including the domain name, server IP address, share name, and the directory where the Network Controller may store data.

e. Time Servers - The system shall support the use of network time servers. Up to three time servers can be designated. Use of a network time server ensures that

the Network Controller and its nodes will be regularly synchronized with the exact time used by all other network resources.

f. A system user holding “Setup” User Role shall be able to configure network resources.

12. LDAP/SLDAP - It shall be possible to configure an Active Directory Server with the S2 SMS.

a. This shall provide single user-login capability.

b. Password rules and authentication will be governed by the LDAP server.

13. Data Operations:

a. View – Users having the “Data Operations: View” user role permission shall be able to view the results of data operations. Depending on which other user permission roles assigned to them, they may also be able to add person records (including access level, credential, and user defined person record information) to the SMS, and modify and delete existing person records.

b. Import File – Shall enable the user to manually upload (import) tab-separated or comma-separated (CSV) text files.

c. Export File – Shall enable the user to manually download (export) CSV text files.

d. Automatic Import – Shall enable the system to process an Import File at scheduled intervals from a pre-configured NAS location.

e. Application Programming Interface (API) – Shall provide the user interface to import CSV data to the SMS. The API shall also be the interface for exporting the entire set of current access level and credential configuration of existing person records from a SMS to an external target system.

2.7 VIDEO MANAGEMENT SYSTEM INTEGRATION

A. General: The SMS shall support the integration of certain Network Video Recorders (NVR). This integration shall allow the viewing of live streaming video in the browser interface and recorded video playback. Viewing live streaming video shall require the Java™ 2 Runtime Environment version 1.4.2 or version 5.0.

1. Events in the alarm subsystem can initiate video recording. Video motion detection, camera up and camera down messages from the VMS can initiate alarms.

2. It shall be possible to monitor DVR and NVR cameras in the same views as IP cameras. VMS events shall be logged in the system activity log. It shall be possible to view recorded video of events from the Activity Log.

3. It shall be possible to view live cameras through floor plans, on the camera view pages, on the Monitoring and Widget Desktops.

4. It shall be possible to pull up recorded video through reports.

B. NetVR Appliances (NetVR and NetBoxVR):

1. NetVR appliances must integrate with Security systems access control, event monitoring, and video management into a single user interface for: live viewing, forensic searching and video exporting.

2. Shall support video surveillance features, including:

   a. Real-time surveillance video integrated on the home page, the Monitoring Desktop, and the Widget Desktop

   b. Viewer-adjustable single camera and multi-camera views (2x2 or 1+7), presets, and camera tours

   c. Calling up cameras through events and through floor plans

   d. Adjust camera with PTZ controls, enabled through UI controls, using mouse or joy stick

   e. Adjust video quality and frame rate in video viewer

   f. Browse video from anywhere that has permitted access to the network and has the accelerator installed

   g. Displays a blue border when there is motion in the frame

   h. Provides the ability to organize surveillance tools using favorite cameras, camera categories, and change sort order.

   i. Can build cases by saving multiple clips into a case file, which is then cataloged in the case library

   j. Clip view displays all the clips in a case

   k. Can print individual frames, including metadata and implied data

   l. Create, save, and export clips of interest

   m. Can export clips in proprietary format with a digital signature, or as AVI file with included video player provided

   n. Allows video searches using the metadata within the Forensic Activity Log, such as searching for events related to a person or a portal.

   o. Supports Codecs, H.264 and MJPEG.

2.8 REMOTE LOCKSET INTEGRATION

A. The SMS shall support the integration of ASSA ABLOY Wi-Fi enabled locksets (models v.S2, p.S2, and IN120) and PoE locksets (models v.S1 and p.S1) with the SMS.

1. The system shall support more than 500 remote locksets; each S2 controller configuration shall be rated for the number of locksets it can support.

2. Once a lockset is installed and registered with the controller, it appears in the security application as a “remote lockset” node, which can be enabled and configured to work with the controller.

3. When a remote lockset connects to the controller, it shall report its power type, which is encoded in its serial number.

    a. A lockset reporting having PoE or direct hardwired power shall be treated as an online lockset and assigned the Default (Online) lockset profile.

    b. A lockset reporting having only batteries as a power source (such as a Wi-Fi lockset) shall be treated as an offline lockset and is assigned the Default (Offline) lockset profile.

    c. The offline remote lockset shall update the controller with the current voltage level of its battery upon each connection.

    d. Clearing the “Online” check box on the Advanced tab of the Network Nodes page will change an online lockset communication status to offline.

    e. The default lockset profile automatically assigned to the lockset the first time it connects to the system shall be editable.

4. It shall be possible to set configuration options for a remote lockset to change its call-in and unlock behaviors.

5. It shall be possible to configure the reader and portal that were automatically created for a remote lockset.

6. It shall be possible to view cached information for a remote lockset, for troubleshooting purposes.

7. It shall be possible to specify special-use formats for access cards to be used with remote locksets.

8. The remote lockset shall be able to send high priority events to the controller.

9. It shall be possible to schedule an automatic unlock period for remote-lockset portals. The start of this period can be triggered by time or by an initial valid card read.

10. It shall be possible to select a check box when creating a magnetic stripe ABA Track 2 card format to ensure that the format will be recognized by remote locksets with magnetic stripe card readers**.**

11. It shall be possible to create remote lockset profiles to assist in the configuration and management of large numbers of remote locksets. A lockset profile is a defined set of attributes that affect lockset behaviors. Assigning a profile to a lockset gives it the attributes defined in the profile. Any subsequent changes made to the profile are applied to the lockset automatically.

12. Locksets shall support PIN-only credentials.

13. It shall be possible to specify a voltage level below which an offline lockset will go into power saving mode. If a Low Battery event is enabled for the lockset, the event will be

triggered. Once the battery is replaced, the lockset will leave power saving mode only when the voltage level reaches 1.5 volts higher than its current Low Voltage setting.

14. It shall be possible for a lockset to check for permissions with the host (controller) for a person that is not yet stored in the lockset.

15. Online locksets shall have the same capabilities as offline locksets with the following additional capabilities:

    a. Online locksets can be assigned to locations; changes to a location's threat level can cause the locksets in that location to enter and exit panic mode.

    b. Online locksets shall have momentary unlock capability while in panic mode (by means of an event action or button on the portal status page).

    c. Online locksets shall be capable of persistent unlock or lock mode (by means of an event action or button).

    d. Online locksets can be added and managed in floorplans.

    e. Online locksets can be unlocked momentarily via event actions or from the Portal Status page, the Widget Desktop, the Monitoring Desktop, or a floorplan.

    f. Online locksets shall be capable of performing scheduled locks or unlocks via, event actions, or from buttons on the Portal Status page, the Widget Desktop, the Monitoring Desktop, or a floorplan.

    g. Online locksets shall be capable of being switched to a locked or unlocked state, and be disabled or enabled using buttons on the Portal Status page.

    h. Online locksets shall be capable of being enabled and disabled via buttons on the Portal Status page.

    i. Activity associated with an online lockset can be viewed in real time in the Activity Log.

2.9 MOBILE SECURITY OFFICER™ APPLICATION

A. The Mobile Security Officer™ (MSO) shall be a mobile application for use with Apple iPad tablets running iOS7.1. The MSO shall enable wireless tablet users to monitor and control various features of the SMS.

1. Activity Monitoring – Users shall be able to view recent activity from the SMS activity log. Users shall be able to select specific activity log entries to view associated records, such as person record details, play live and recorded video, and change the status of specific portals.

2. View Person Details – Users shall be able to search for persons by name, and view associated person records. Users shall be able to photograph persons using the camera on their tablet, and record these in the SMS.

3. Live Video Monitoring – Users shall be able to display thumbnail images of every NetVR camera view integrated with the SMS. Users shall be able to select individual thumbnails, which shall display live video from the corresponding camera.

4. Mobile Mustering - The application shall support a mustering process using a mobile device to allow regional evacuation, unimpeded by access control constraints. Users shall be able to initiate and terminate multiple evacuations simultaneously. The system shall enable users to determine if all persons known to be present within a given region have been accounted for. The system shall be capable of managing mustering points simultaneously.

5. The MSO shall support up to five simultaneous iPad connections per Controller.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Examine existing cable pathways including conduit, raceways, cable trays, and other pathway elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

B. Examine rough-in for control cable and conduit systems to controllers, card readers, and other EACS components to verify conduit and back-box locations prior to installation of EACS devices

C. Examine available network capacity and support infrastructure. Consult with network administrator for compliance with network standards and capacity.

D. Examine install location for compliance with space allocations, installation tolerance, hazards to safe system operation, and other conditions affecting installation.

E. Examine roughing-in for LAN, WAN, and IP network before device installation.

F. Proceed with installation only after unsatisfactory conditions have been corrected.

3.2 PREPARATION

A. Comply with SIA CP-01 Control Panel Standard.

B. Comply with ANSI/TIA-606-B Labelling Standard.

C. Prepare detailed project planning forms for programming and configuration of the SMS. Fill in all data available from project plans and specifications and publish as project planning documents for review and approval. These may include (but are not limited to):

1. Define SMS Partitions.

2. For each Location, record setup of controller features and access requirements.

3. Propose start and stop times for time zones and holidays, and match up access levels for doors.

4. Set up groups, facility codes, software triggers, and list inputs and outputs for each controller.

5. Assign action message names and compose messages.

6. Set up alarms. Establish trigger actions between events and video surveillance features.

7. Prepare and install alarm graphic maps.

8. Develop user-defined fields.

9. Develop screen layout formats.

10. Discuss badge layout options; design badges.

11. Complete system diagnostics and operation verification.

12. Prepare a specific plan for system testing, startup, and demonstration.

13. Develop acceptance test concept and, on approval, develop specifics of the test.

14. Develop cable and asset-management system details; input data from construction documents. Include system schematics and technical drawings in electronic format.

D. In meetings with Architect and Owner, present Project planning documents and review, adjust, and prepare final programming and configuration documents. Use final documents to program and configure SMS software.

3.3 CABLING

A. Comply with NECA 1, "Good Workmanship in Electrical Construction".

B. Install cables and wiring according to industry standards "Conductors and Cables for Electronic Safety and Security

C. Wiring Method: Install wiring in raceway and cable tray except within consoles, cabinets, desks, and counters. Conceal raceway and wiring except in unfinished spaces.

D. Install LAN cables using techniques, practices, and methods that are consistent with Category [5E OR 6] rating of components and fiber-optic rating of components, and that ensure Category [5E OR 6] and fiber-optic performance of completed and linked signal paths, end to end.

E. Junction boxes and enclosures containing security-system components or cabling, and which are easily accessible to employees or to the public, shall be provided with tamper resistant fasteners and/or tamper detection switches. In addition, hinged enclosure doors shall be equipped with locking hardware. Boxes above ceiling level in occupied areas of the building shall not be considered accessible. Junction boxes and small device enclosures below ceiling level and easily accessible to employees or the public shall be covered with a suitable cover plate and secured with tamperproof screws.

F. Install end-of-line resistors at the field device location and not at the controller or panel location.

3.4 CABLE APPLICATION

A. Comply with TIA 569-C, "Commercial Building Standard for Telecommunications Pathways and Spaces."

B. Card Readers and Keypads and Peripheral Devices:

1. Install number of conductor pairs recommended by device manufacturer for the functions specified.

2. Follow device manufacturer's installation requirements for maximum cable distances and sizes.

3.5 GROUNDING

A. Comply with IEEE 1100, "Recommended Practice for Power and Grounding Electronic Equipment."

B. Ground cable shields, drain conductors, and equipment to eliminate shock hazard and to minimize ground loops, common-mode returns, noise pickup, cross talk, and other impairments.

C. Signal Ground:

1. Terminal: Locate in each equipment room and wiring closet; isolate from power system and equipment grounding.

2. Bus: Mount on wall of main equipment room with standoff insulators.

3.6 IDENTIFICATION

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

1. All wiring conductors connected to terminal strips shall be individually numbered, and each cable or wiring group being extended from a panel or cabinet to a building-mounted device shall be identified with the name and number of the particular device as shown.

B. At completion, cable and asset management documentation shall reflect as-built conditions.

3.7 SYSTEM SOFTWARE AND HARDWARE

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

3.8 FIELD QUALITY CONTROL

A. Perform tests and inspections:

1. Manufacturer's Field Service: Engage a factory-authorized S2 service representative to inspect components, assemblies, and equipment installations, including connections, and to assist in testing.

2. Factory Commissioning: Onsite visit by the Manufacturer's in-house personnel to inspect, test, and assess system programming, functionality, and performance

B. Tests and Inspections:

1. LAN Cable Procedures: Inspect for physical damage and test each conductor signal path for continuity and shorts. Test for faulty connectors, splices, and terminations. Test according to TIA/EIA 568-C, "Commercial Building Telecommunications Cabling Standards - Part 1: General Requirements." Link performance for UTP cables must comply with minimum criteria in TIA/EIA 568-C.

2. Test each circuit and component of each system. Tests shall include, but are not limited to, measurements of power-supply output under maximum load, signal loop resistance, and leakage to ground where applicable. System components with battery backup shall be operated on battery power for a period of not less than 10 percent of the calculated battery operating time. Provide special equipment and software if testing requires special or dedicated equipment.

3. Operational Test: After installation of cables and connectors, demonstrate product capability and compliance with requirements. Test each signal path for end-to-end performance from each end of all pairs installed. Remove temporary connections when tests have been satisfactorily completed.

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

D. Prepare test and inspection reports.

3.9 STARTUP SERVICE

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

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

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

3.10 ADJUSTING

A. Occupancy Adjustments: When requested within 30 days of date of Substantial Completion, provide on-site assistance in adjusting system to suit actual occupied conditions. Provide up to two visits to Project for this purpose. Tasks shall include, but are not limited to, the following:

1. Check cable connections.

2. Check proper operation of card readers, intrusion sensors, integrated systems, and database configuration. Verify SMS configuration and adjust settings needed.

3. Recommend changes to SMS configuration and settings to improve Owner's use of SMS.

4. Provide a written report of adjustments and recommendations.

3.11 Existing equipment

A. A new door access computer is to be supplied and the existing unit to be turned over to the owner.

B. Lock power supplies are to be changed and old units turned over to the owner. The new lock power supplies are to be based on Altronix AL400 with battery back-up. They are to be sized with 20% future expansion.

C. Door contacts and Request to exit motions can be reused only if they have been checked verified that the properly work and will be included in the first year warrantee.

D. Card reader will be HID I Class based on 920PTNNK000. Included in this project will be (100) access cards to be used with the system. They are to be programed to the Simsbury Water Treatment personnel and turned over to the owner.

E. The existing building intrusion system is currently integrated in with the existing door access system. A new system based on Honeywell Vista system must be installed to replace it. Existing security devices can be reused only if they have been checked verified that the properly work and will be included in the first year warrantee.

F. Offsite monitoring account.

G. The main gate currently is controlled by the door access system. However it only controls one side of the gate. The new system must control both sides of the gate. The owner will let the installing contractor know the sequence of controlling both sides of the gate.

APPENDIX 2
WPCA Facility Layout

Security Access Controls Update

History: The original door access card reader system (TOPAZ) was manufactured by GE Security. As a result of an acquisition GE Security no longer supports TOPAZ.

Scope:

1. The current TOPAZ software is no longer supported and must be replaced. The system computer has failed.
2. The following figure identifies the Security Access Control Panels and readers.

On review, the system includes (25) Card readers, (40) Door contacts and (14) Glass break detectors. All existing wiring will be re-used along with existing card readers and electric locking devices. Winning bidder will supply a computer workstation to be used by the door access system that will include a desk computer and monitor.

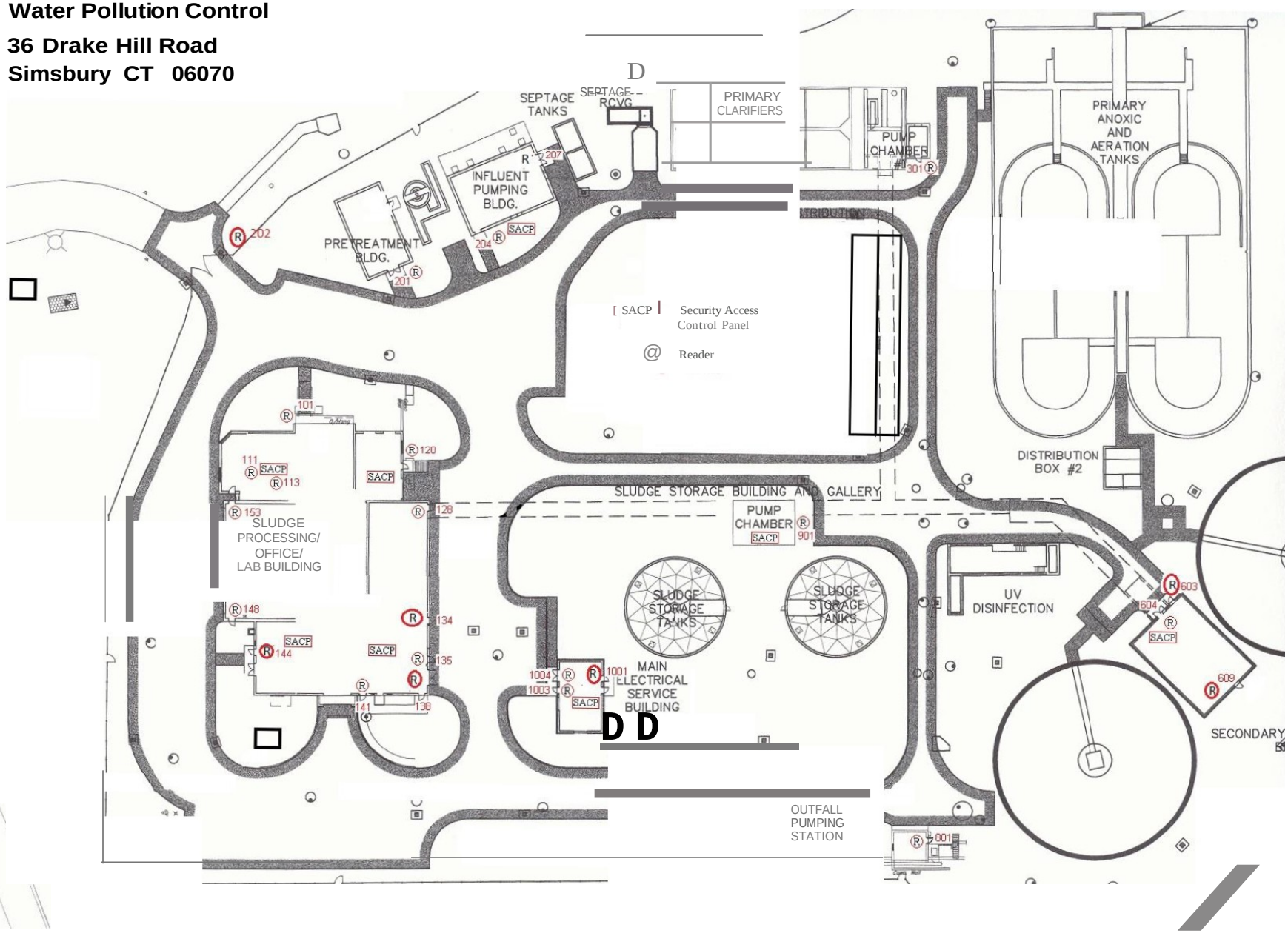
Table 1: Access Card Reader Locations

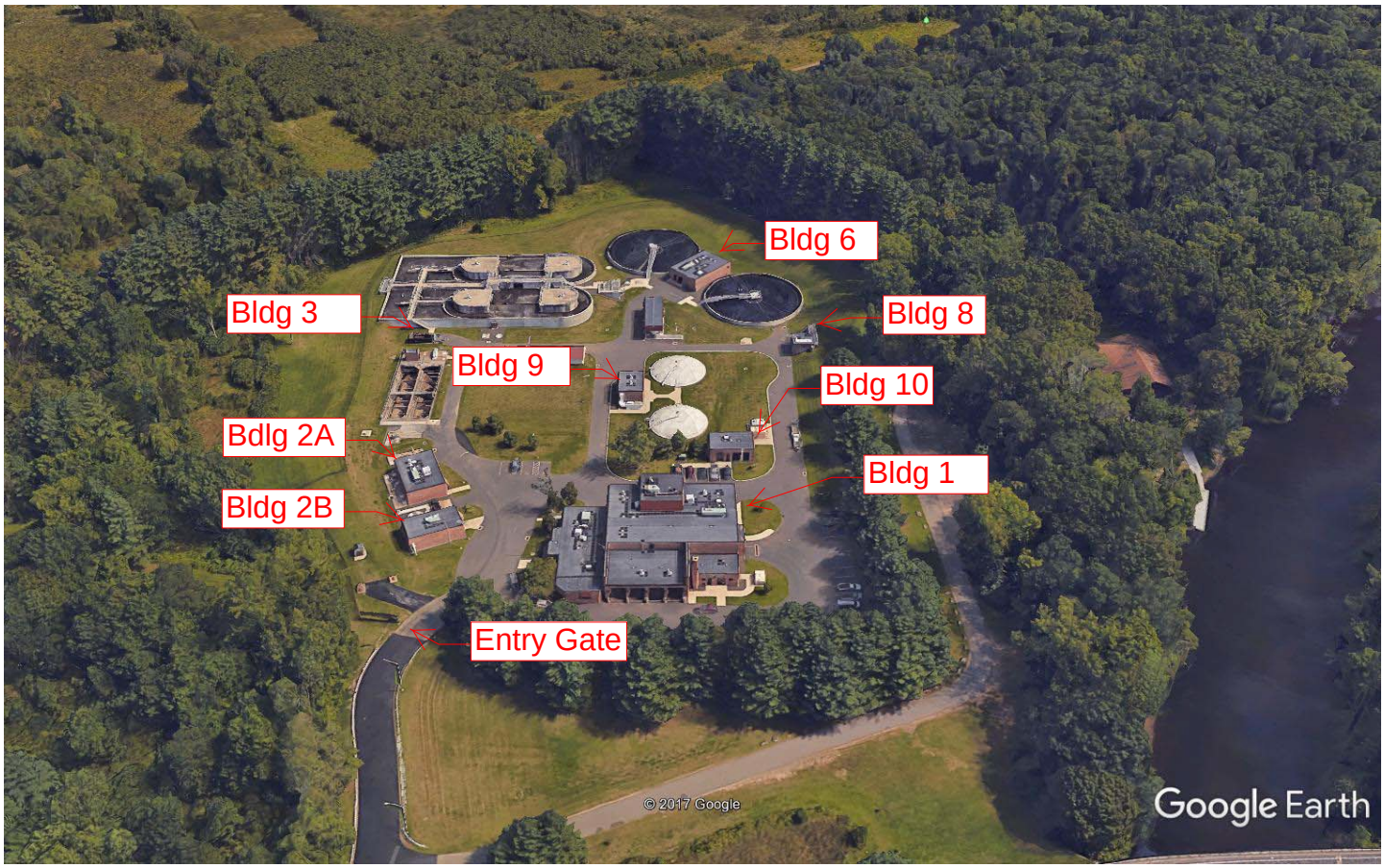
Security Access Control	Reader Name	Door No.
BOILER ROOM 1-1	BOILER RM DR	144
	GR DR EAST	148
	GR DR WEST	152
	RDR 1-1-2	
BUILDING 10 1-2	BLD 10 NO	1001
	BLD 10 S/E	1003
	BLD 10 S/W	1004
	RDR 1-2-3	
BUILDING 2 1-4	BLD 2B DBL	207
	BLD 2B SING	204
	BLD 2A FRNT	201
	GATE	202
BUILDING 6 1-6	BLD 6 REAR D	609
	BLD 6 S/E	603
	BLD 6 S/W	604
	BLD 8 DOOR	801
BUILDING 9 1-5	BLD 9 DOOR	901
	PUMP CHAMBER	301
	RDR 1-5-2	
	RDR 1-5-3	
CONTROL ROOM 1-0	FRONT DOOR	101
	OFFICE DOOR	111
	RDR 1-0-1	
	REAR OFF DR	113
GARAGE 1-7	SHOP DOOR	134
	SLUDGE BAY	141
	STAIR ENT	135
	WORK SHOP	138
TELEPHONE CLOSET 1-3	GR DR N/W	128
	RDR 1-3-1	
	RDR 1-3-3	
	REAR DR N	120
	Total Readers	25

Water Pollution Control

36 Drake Hill Road

Simsbury CT 06070





Google Earth

feet 400
meters 100