

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT			1. Contract Number	Page of Pages	
				1	63
2. Amendment/Modification Number	3. Effective Date	4. Requisition/Purchase Request No.		5. Solicitation Caption	
GF-2012-B-0033-003	December 19, 2011			Renovation of Student Services Center, Building 39, Level A	
6. Issued By:		Code	7. Administered By (If other than line 6)		
University of the District of Columbia Capital Procurement Division 4200 Connecticut Avenue, NW, Room C03 Building 38 Washington, DC 20008			University of the District of Columbia Capital Procurement Division 4200 Connecticut Avenue, NW, Room C03 Building 38 Washington, DC 20008		
8. Name and Address of Contractor (No. Street, city, country, state and ZIP Code)			(X)	9A. Amendment of Solicitation No.	
				GF-2012-B-0033	
				9B. Dated (See Item 11)	
				November 21, 2011	
				10A. Modification of Contract/Order No.	
				10B. Dated (See Item 13)	
Code	Facility				
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS					
<input checked="" type="checkbox"/>	The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers <input checked="" type="checkbox"/> is extended, <input type="checkbox"/> is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning <u>1</u> copy of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or fax which includes a reference to the solicitation and amendment number. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or fax, provided each letter or telegram makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.				
12. Accounting and Appropriation Data (If Required)					
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14					
A. This change order is issued pursuant to: (Specify Authority)					
The changes set forth in Item 14 are made in the contract/order no. in item 10A.					
B. The above numbered contract/order is modified to reflect the administrative changes (such as changes in paying office, appropriation date, etc.) set forth in item 14, pursuant to the authority of 27 DCMR, Chapter 36, Section 3601.2.					
C. This supplemental agreement is entered into pursuant to authority of:					
D. Other (Specify type of modification and authority)					
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input checked="" type="checkbox"/> is required to sign this document and return <u>1</u> copy to the issuing office.					
14. Description of amendment/modification (Organized by UCF Section headings, including solicitation/contract subject matter where feasible.)					
Solicitation No. GF-2012-B-0033 for Renovation of Student Services Center, Building 39, Level A, is hereby amended as follows:					
1. Additional Questions and Answers (Attachment A);					
2. Pre-Bid Conference Sign-In Sheet (Attachment B);					
3. Plan Holders List (Attachment C);					
4. Clarifications/Supplemental Information (Attachment D);					
5. Interior Signage (Attachment E);					
6. Fabric Wrapped Layout Sketch (Attachment F);					
7. Operable Partition Sound Baffle Detail (Attachment G);					
Except as provided herein, all terms and conditions of the document referenced in Item (9A or 10A) remain unchanged and in full force and effect					
15A. Name and Title of Signer (Type or print)			16A. Name of Contracting Officer		
			SHERRY JONES-QUASHIE		
15B. Name of Contractor		15C. Date Signed	16B. District of Columbia		16C. Date Signed
			<i>Sherry Jones-Quashie</i>		12/19/11
(Signature of person authorized to sign)			(Signature of Contracting Officer)		

**Renovation of Student Services Center, Bldg. 39, Level A
GF-2012-B-0033**

8. Dumpster Location Image (Attachment H);
9. Access Panel Images (Attachment I);
10. Corridor Fire Rating Sketch (Sht. G0.03) (Attachment J);
11. OFFICE OF PUBLIC SAFETY/POLICE University of the District of Columbia Integrated Security Management Specifications (Attachment K);
12. A third site visit to see additional disposal requirements has been scheduled for Tuesday, December 20, 2011 at 11:00 AM;
13. The bid opening date is hereby extended from Wednesday, December 21, 2011, 2:00 PM to Thursday, December 22, 2011, at 2:00 PM;
14. All other terms and conditions remain unchanged.

ATTACHMENT A

Renovation of Student Services Center, Bldg. 39, Level A
GF-2012-B-0033

Additional Questions and Answers

- (1). **Question:** The specified manufacturer for the operable partition is stating that: "We do not install non electric AS933 continuously hinged partition, but would recommend our AS932 series as an alternative. And the specification calls for a 41 STC MDF surfaces partition. This is extremely low, and does no more than a sight divider. Is the client sure about this rating?" Please provide us a response ASAP.
- Answer:** Basis-of-design model shall be **Modernfold Inc, Acousti-Seal 932** However equivalent substitutions will be considered. This is a paired panel system, a continuously hinged partition is not specifically required. Operable partitions shall be manually operated as described in Spec 10650, 2.1 and 2.2. **STC 52** rating required, steel facing acceptable.
- (2). **Question:** Please provide the following missing specification sections: Signage – Drawing A1.04; Prefinished metal cover on existing column – Drawing A5.61A
- Answer:** Interior room signage shall be provided as detailed in Sht. A1.04 for size and content. Material, color, font type, shall meet UDC standard (see attached specification section 10443 included in this Amendment). Prefinished metal columns shall be flush joint, prefinished aluminum as manufactured by the following: Pac-Clad, Fry-Reglet, Doralco, Pittcon, or equal. (**Attachment E**)
- (3). **Question:** Drawing D1.01 doesn't show ceiling demolition. Drawing A1.02 shows new ceiling. Do we need to demo existing ceiling? Please advise and provide the drawing for existing ceiling demolition.
- Answer:** Refer to Sht. D1.01 General Note 8. All existing ceiling assemblies in area of renovation scheduled to receive new ceiling to be removed.
- (4). **Question:** Does the mechanical system need to tie-in to the existing building control system? If so, please provide the name of the existing building control system.
- Answer:** Tie-in to existing building control system is not part of the scope.
- (5). **Question:** There is a specification section 09771 – Fabric-Wrapped Panels, but the drawings don't show where to use these panels (room location, interior elevation of that room, size of panels, quantity of panels) and how to install these panels (cross section details). Please advise

Renovation of Student Services Center, Bldg. 39, Level A
GF-2012-B-0033

Answer: Partition surfaces required to receive fabric-wrapped panels are designated as WC-1 on finish schedule. They are specified for the Conference Rm. 107/108. Panels shall be placed as depicted in sketch and mounted utilizing the manufacturer's recommended clip attachment system. **(Attachment F)**

(6). **Question:** Drawing A4.01, key note #9 shows freestanding, floor mounted, prefabricated CPU kiosk unit. Do we need to furnish and install CPU kiosk unit? If so, please provide the drawing details and specification for CPU kiosk unit

Answer: Kiosk units have been **removed** from the scope of work and will be part of a separate FFE package. Contractor to provide wiring/ cabling and connections as shown in the electrical/data drawings for future installation.

(7). **Question:** Drawing detail 1/A6.01 shows the recommended sound baffle by others. Is this item part of the scope of work? If so, please provide the specification for the sound baffle

Answer: Sound baffle will consist of framed drywall assembly as required to maintain acoustical separation of operable partition. **(Attachment G)**

(8). **Question:** Drawing FF1.01 has a general note #1 "*All furnishings shown for location only. Furnishing to be specified & purchased by Owner.*" Please confirm if this is correct.

Answer: Correct. Systems and freestanding furniture are not in the contractor's scope.

(9). **Question:** Detail 1/A6.01 states, "*Contractor to submit engineering shop drawings including structural support above receiving operable partition mounting.*" This mounting structural detail should be provided by the on-boarded designers, and not by the Contractor. Therefore, please provide a mounting structural detail so we can price the appropriate cost.

Answer: Structural support for the operable partition typically consists of a steel framing and shall be determined by the final weight, operating loads, and system type of the product selected and approved for installation. Therefore the structural support for the operable partition shall be submitted by the contractor as indicated in Spec section 10650, 1.4, D as part of the construction submittal. If requested, the operable partition manufacturer may include this design as part of their submittal preparation package.

Renovation of Student Services Center, Bldg. 39, Level A
GF-2012-B-0033

(10). **Question:** Will classes be in session during the construction period?

Answer: Classes will be in session during construction.

(11). **Question:** Where is the dumpster lay down area? Can we use the exit doors to the east side deck or do we need to go through the lobby to get to dumpster lay down area? Please advise.

Answer: See the following:

1. Contractor is to provide tree protection at the drip line of all trees.
2. Do not block access to Fire Department connection.
3. Protect all pavers and curbs.
4. Protect all underground utilities.
5. Repair to original condition any damage caused by the Contractor.
6. Restore grass and landscaping to original condition when finished.

(Attachment H)

ATTACHMENT B

SOLICITATION NO.: GF-2012-B-0033

Renovation of Student Services Center at Building 39
 Thursday, December 1, 2011 - 1:30 PM - Building 39, Third Floor, Large Board Room

PRE-BID CONFERENCE SIGN-IN SHEET

PLEASE PRINT

NO	NAME	COMPANY	TELEPHONE NO.	EMAIL ADDRESS
1	N.V. Satish	NVS CONSTN Co	2-216-9883	nvsconst@verizon.net
2	Eric Scott	Trinity II	2-704-8337	ebscott@gmail.com
3	ALEX VALENZUELA	NASTOS Construction	202-348-5500	ALEX.VALENZUELA@NASTOS.CO
4	John Carner	Hopeday Construction	202-316-0006	jcarner@hopedayimprovements.com
5	SANDERS HOWFU	ESI WASTE	671-230-1339	THOWFU@ESIWASTE.COM
6	JOHN HAUSER	BENNETT GROUP	202-625-3330	JHAUSER@BENNETTGROUP.COM
7	Ike Okunmabus	Simon Devel. & Const. Corp	202-829-3316	Simoncc@verizon.net
8	KROSTEL	THE LEXX GROUP INC.	202-393-3085	KROSTEL@THELEXXGROUP.COM
9	Ted yim	CHY Contracting inc	703-378-8190	tedyim@chcontracting.com
10	Jeff Pritz	CCC	202-562-0027	estimating@cc-builder.com
11	Parker Goodsell	POUNDS	301-998-8863	parker@pounds.com
12	Pritesh Shah	FEI Construction	202-529-2140	pritesh@forneyent.com
13	Y.R. Kasimsetty	CONSUS, INC.	2545 1333	vijay@consus-inc.net
14	James McCall	United General Contractors Inc	2526-2101	unitedflash@aol.com
15	SHOD AKINYE	GENERAL SERVICES, INC	2-545-0127	info@gsidc.washdc.com

SOLICITATION NO.: GF-2012-B-0033

Renovation of Student Services Center at Building 39
 Thursday, December 1, 2011 - 1:30 PM - Building 39, Third Floor, Large Board Room

PRE-BID CONFERENCE SIGN-IN SHEET

PLEASE PRINT

NO	NAME	COMPANY	TELEPHONE NO.	EMAIL ADDRESS
16	Kolar Bowen	Bennett Group	625-3330	kbowen@bennettgroupdc.com
17	Calvin Reid	Atlas Mfg Inc.	(202) 562-5330	clreid@atlasman.net
18	GREEN PRINT INC	BILAL AZIZ	703-731-0457	baziz@ats-worldwide.com
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

SOLICITATION NO.: GF-2012-B-0033

Renovation of Student Services Center at Building 39
 Thursday, December 1, 2011 - 1:30 PM - Building 39, Third Floor, Large Board Room

PRE-BID CONFERENCE SIGN-IN SHEET

PLEASE PRINT

NO	NAME	COMPANY	TELEPHONE NO.	EMAIL ADDRESS
46	CAROLINE BALDWIN	JACOBS/UDC	202-274-1886	caroline.baldwin@udc.edu
47	Alex Garrett	UDC	202-274-5353	ajgarrett@udc.edu
48	EDGAR MORENO	SORG ARCH	202-393-6415	EDGAR.MO@SORGARCHITECTS.COM
49	Surinder Khanna	Const Mgrs/Jacobs/UDC	703-400-4834	S.Khanna@UDC.edu
50	Alvin D VEWSON	UDC	202-274-6361	AVENSON@UDC.EDU
51	Sherry Jones-Quelin	UDC	202-274-5752	Sherry-Quelin@UDC.EDU
52	Carolee J. Moody	UDC	202-274-5774	cmoody@udc.edu
53	Tamara Phelps	UDC	(202) 274-6721	tphelps@udc.edu
54				
55				
56				
57				
58				
59				
60				

ATTACHMENT C



CAPITAL PROCUREMENT DIVISION

Supplier Mailing List (for Pick-up of Solicitations)

Issue Date: _____
 Solicitation Number: GF-2012-B-0083
 Caption: Renovation of Student Services Center at Bldg 39, Level A

Opening Date: 11/2/11 Closing Date: 12/2/11
 Opening Time: _____ Closing Date: _____

Date: 11/29/2011

FEI CONSTRUCTION CO.
 A Division of Forney Enterprises, Inc.

PRITESH SHAH
 Office Engineer

1818 New York Ave., NE, Suite 201
 Washington, DC 20002
 Email: pritesha@forneyent.com

202-529-2140
 Fax 202-529-2377

Date: 2/1/11 2

Company Name: NVS CONSTN CO

Contact Person: N.V. SATISH

Address: 10701 4th St NW
SPE 307, DE 20004

Phone No: 202 216 0183
 Fax No: 202 216 0183

Email Address: pritesha@verizon.net

Date: 11/29/2011

POUNDS

Nick Hunter

500 H Street NE, Suite 31
 Washington DC 20002
 T 202 543 9431
 F 202 280 1263
 C 703 867 5002
 nick@poundsdc.com
 www.poundsdc.com

Date: 12/1/11

Company Name: CHU Contracting, Inc

Contact Person: Ted Yun

Address: 14111 Marian Ct
Chantilly, VA 20151

Phone No: 703-378-8196
 Fax No: 703-378-8191

Email Address: ted.yun@chuccontracting.com

THE LEXX GROUP INC.
 General Contracting - Construction Management - Design/Build

Kenneth D. Postell
 President /CEO

400 5th Street NW Suite 400
 Washington, DC. 20001
 kpostell@thelexxgroup.com
 www.thelexxgroup.com

Office 202.393.3085
 Fax 202 393 3089
 Direct 202 787 9800

Email Address: 12/1/11

Date: 12/1/2011

Company Name: CONSYS, INC

Contact Person: Vijay Kasimsetty

Address: 732 Kennedy St. NW
Washington DC 20011

Phone No: (2) 545 1333
 Fax No: (2) 545 1339


Email Address: vijay@consys-inc.net

CAPITAL PROCUREMENT DIVISION

Supplier Mailing List (for Pick-up of Solicitations)

Issue Date:	Opening Date: <u>11/21/11</u>	Closing Date: <u>12/21/11</u>
Solicitation Number: <u>BF-2012-B-0033</u>	Opening Time: _____	Closing Date: _____
Caption: <u>Remediation of Student Services Center at Bldg. 39, Level A</u>		

Date: 12/1/11



GENERAL SERVICES, INC.
Construction Management, General Construction, Facility Mgmt.
Design & Build

8(a) • Hubzone • CBE/LSDBE • WOMEN OWNED

Date: 12/02/2011

Company Name: Simon Development & Const. Con

Contact Person: Ikego Okulimabua


Address: 7600 Georgia Ave. NW
Suite 409, Washington, DC 20012

Phone No: 202-829-3316

Fax No: 202-809-0146

Email Address: simoncc@verizon.net

Date: 12/1/11



Alex Valenzuela
Project Manager

1121 Kashiwanke Ave. NE, Washington DC 20002
Phone: 202.546.5500 Ext 123 Fax: 202.546.5500
Cell: 202.546.5500
http://www.princeconstruction.com

Date: _____



Michael Sigal
President
LEED® Green Associate

1800 M St. NW | Suite 1050 South | Washington, DC 20036
202.944.6600 main | 202.944.6681 direct
202.437.6667 mobile | 202.944.6620 fax
msigal@gcs-dc.com | www.gcs-dc.com | Twitter: @msgcs


Date: 12/2/11



Herber Beltran
Estimator/ Project Manager
1111 Good Hope Road, SE
Washington, DC 20020
202-889-5050
202-409-6377 Cell
202-610-4497 Fax

herber.beltran@princeconstruction.com
Prince Construction Company, Inc.
Certified: D.C. LSDBE-MDOT-VDOT-WMATA-MWAA-P.G. MBOC

Date: 12-5-11



eeci incorporated



3303 Hubbard Road
Lanndon, Maryland 20785
toll free 800.372.3728
local 301.341.1000
facsimile 301.341.1009
web eeciinc.com

CAPITAL PROCUREMENT DIVISION

Supplier Mailing List (for Pick-up of Solicitations)

Issue Date: _____ Solicitation Number: <u>BE-2012-B-0133</u> Caption: <u>Renovation of Student Center Services at Bldg. 39, Level A</u>		Opening Date: <u>11/21/11</u> Opening Time: _____	Closing Date: <u>12/1/11</u> Closing Date: _____
Date: <u>12/9/11</u> Company Name: <u>Construction Software Technologies, Inc</u> Contact Person: <u>Kevin Turlow</u> Address: <u>5542 Nicholson Lane</u> <u>Rockville MD 20852</u> Phone No: <u>800-364-2059</u> Fax No: <u>866-570-8187</u> Email Address: <u>washdc@isgft.com</u>	Date: <u>12/9/11</u> Company Name: <u>MC-GRAW HILL</u> Contact Person: <u>Margaret Stone</u> Address: <u>3315 Central Avenue</u> <u>Hot Spring AR 71913</u> Phone No: <u>607-708 8055</u> Fax No: <u>586 279 4450</u> Email Address: <u>vicki_proulx@mcgraw-hill.co</u>		
Date: <u>12.14.2011</u> Company Name: <u>Compass Solutions LLC</u> Contact Person: <u>Emmanuel Agborfo</u> Address: <u>1401 K Street NW ste 802</u> <u>Washington DC</u> Phone No: <u>240 898 7317</u> Fax No: _____ Email Address: <u>eagborfo@compasscentral.com</u>	Date: <u>12/15/11</u> Co: _____ Co: _____ Ad: _____ Ph: _____ Fa: _____ Err: _____		
Date: <u>12-15-11</u> Company Name: <u>Horton & Barber</u> Contact Person: <u>PAUL Horton</u> Address: <u>3127 MHC J, Ave SE</u> <u>WASHINGTON</u> Phone No: <u>202-373-0433</u> Fax No: <u>202-373-0633</u> Email Address: <u>hortonbarber@com-const.net</u>	Date: _____ Company Name: _____ Contact Person: _____ Address: _____ Phone No: _____ Fax No: _____ Email Address: _____		



MICON
CONSTRUCTIONS

(A Design, Build & Development Co.)
8(a)/SDB

1818 New YORK AVENUE, NE
Suite 218
Washington, DC 20002

Steve Gray
Director of Operations

ph 202.636.3930
fx 202.636.3931
e info@miconconstruction.com

CAPITAL PROCUREMENT DIVISION

Supplier Mailing List (for Pick-up of Solicitations)

Issue Date: _____
 Solicitation Number: GF-2012-13-0033
 Caption: Renovation of Student Center Services at Bldg. 39, Level A

Opening Date: 11/21/11 Closing Date: 12/21/11
 Opening Time: _____ Closing Date: _____

Date: 12/5/11

Company Name: TITO Contractors Inc.

7308 Georgia Ave, N.W.
 Washington, DC 20012
 (202) 281-2255
 (202) 726-0495

1658 W North Avenue
 Baltimore, MD 21217
 (410) 462-3200
 (410) 462-4022

Alex Pierola
 Vice President
 (202) 484-4818
 apierola@titocontractors.com



www.titocontractors.com

Date: 12/7/11

Company Name: Monarc Const Inc.

Contact Person: Randy Mullen

Address: 2781 Hartland Road
Falls Church, VA 22043

Phone No: 703-641-8500
 Fax No: 703-641-9794

Email Address: rmullen@monarcconstruction.com

Date: 12/6/11

Company Name: Broughton Construction Company

1050 17th St, Suite 440
 Washington, DC 20036
 O: 202-589-0066
 F: 202-589-0067
 C: 202-558-8838

807 E. Baltimore Street
 Baltimore, MD 21202
 O: 410-244-5508
 F: 410-244-5509
 C: 202-558-8838



VINSON T. STRINGER
 Business Development Coordinator
 vstringer@broughtonconstruction.com

Date: 12/8/2011

Company Name: Chicaramonte Construction

Contact Person: Jeff Plotz

Address: 605 Raleigh Place, SE
Wash. DC 20033

Phone No: 202-562-0072
 Fax No: _____

Email Address: estimating@cc-builder.com

Date: 12/7/11

Company Name: Protec Construction Inc.

Contact Person: Vik Singh

Address: 1314 8th St NW
Washington DC 20001

Phone No: 202-232-0080
 Fax No: 202-232-0092

Email Address: Vik@protecconstructioninc.net

Date: 12/9/11

Company Name: Thoran Real Estate Services

Contact Person: Robert Taylor

Address: 1100 New York Ave NW Suite 700W
Washington DC 20005

Phone No: 202 290 2061
 Fax No: 202 688 1448

Email Address: rtaylor@thoran.com

ATTACHMENT D

Renovation of Student Services Center, Bldg. 39, Level A GF-2012-B-0033

Clarifications/ Supplemental Information

The following items are clarifications and supplemental information to the Bid documents to be included in the contractor's scope of work.

1. Demolition

SHT. D1.01, P2.0 Demolition Plans-

1. All remaining furniture, partitions, door assemblies, equipment and trash remaining in the area of renovation shall be removed.
2. Add Key Note 13 to UDC Campus Police space and adjacent storage room.
3. Add Key Note 12 to center spaces.
4. At CL B.75 and 2, key note refers to art work, it is a glass display case.
5. Security box not shown between the Exit Stair and Men's toilet room shall be removed (Key Note 2).
6. The office at CL B.25 and 5.5 needs Key Note 12.
7. All existing water fountains in the former Children's Play Area shall be removed.
8. Existing security cabling above the former UDC Campus Police area ceiling shall remain.
9. Contractor shall remove existing blinds and brackets within the area of renovation.

2. Existing Infloor Utility Access Panels

Existing floor access panels serving infloor utility ducts are no longer in use. Contractor shall prepare duct access locations with suitable substrates compatible with the flooring material to allow for flush installation of scheduled flooring. Access panels may be filled with concrete or flooring compound (as depths allow), flush with existing slab level. Contractor shall field verify quantities. Similar treatment shall apply to the small access covers throughout the space.

(Attachment I)

3. Ceiling Plans

SHT. A1.02, A4.01, A6.02- Where ceiling plans are depicted in the architectural drawings, refer to MEP drawings for further information regarding placement of lighting fixtures, mechanical, and FA devices. Refer to Finish Schedule on SHT. A6.02 for ceiling finishes. Ceiling info on plan drawings depict scheduled finishes for graphical reference and coordination with adjacent materials.

4. Corridor Fire Rating

SHT. G0.03, A1.01, A6.01- All partitions indicated shall be fire rated and shall be Type 1. Where required to achieve fire rating, Partition Type 1 shall meet UL U465 partition assembly. For additional fire rating requirements pertaining to Rms. 102, 103 (Reception/ Lobby), and 105 (Corridor). Refer to **(Attachment J)**

Renovation of Student Services Center, Bldg. 39, Level A
GF-2012-B-0033

Note- Fire rated Type 1 partitions must be maintained within Lobby partition assemblies where additional furring will be required to form recessed openings.

5. Door Fire Ratings

SHT. A6.03- Per Clarification for No. 4, Corridor Fire Rating above, the following doors are being modified to 20 minute fire rated solid core wood (SCW) door assemblies and shall receive closers: 104, 111, 135, 108, 107, 109, 134, 106, 145.

1. Where sidelites are specified (Door type D5) and indicated on plans, provide minimum 20 minute rated sidelite assembly in lieu of frameless glass. Provide TGP **Firelite Plus** glass system with Designer Series framing or equivalent product to match sizes indicated on A6.03.
2. Door 122 shall be a Type D5 fire rated single door with closer and sidelite.

6. Fire Penetrations/ Fire Dampers

All penetrations thru fire rated assemblies indicated on bid documents and described under No. 4, Corridor Fire Rating above, shall receive UL-classified fire-stop systems. For new ductwork, fire dampers shall be provided at all penetrations thru fire rated assemblies shown under No. 4, Corridor Fire Rating

7. Security Specs/ Door Hardware

Contractor shall provide the following security hardware for the following doors:

1. Doors 111, 122, 134, 135, 145 shall receive electronic access control locksets as manufactured by Salto Systems. See attached UDC Security Specifications.
2. Door 103- Double magnetic locks, reuse existing reader.

Devices shall tie to existing system. All scope related to Security shall comply with the OFFICE OF PUBLIC SAFETY/POLICE, University of the District of Columbia Integrated Security Management Specifications. (**Attachment K**)

8. Electrical/ Communications

SHT. E4.00-

1. Key note 4, Contractor shall provide installation/wiring for ADA access devices.
2. Keynote 5, Contractor shall provide installation/wiring for electric locks and card readers.
3. Provide security locks on seven doors as appropriate and outlined in No. 7, Security Specs/Door Hardware above.
4. Coordinate with UDC reuse of existing servers.

Renovation of Student Services Center, Bldg. 39, Level A
GF-2012-B-0033

SHT. E6.00-

1. Contractor shall provide all telephone and data wiring/cabling. Plates shall be labeled and color coded appropriately and wires/cables labeled.
2. Detail 1 of Data Cover plate- Spare shall receive a blank cover.
3. All existing abandoned wiring/cabling shall be removed and disposed of.
4. Provide additional patch panel(s) in the data rack.

9. Visual Display Surfaces

Conference Rms. 107/108 shall receive four (4) marker boards. Refer to Specification section 10101, Visual Display Surfaces.

10. Roller Shades

Contractor shall provide manual roller shades along existing exterior glazed conditions. Shades shall comply with UDC standard: **North Solar Screen LLC, Verosol Silver Screen, Color-Bronze.**

ATTACHMENT E

SECTION 10443 - NON-ILLUMINATED INTERIOR SIGN MESSAGE PANELS

PART 1 - GENERAL

BID QUESTION #2- INTERIOR SIGNAGE

1.1 SUMMARY

- A. This Section includes interior non-illuminated directional, control, and information surface mounted signage as complete integrated modular system.

1.2 REFERENCES

- A. Standards of the following as referenced:
 - 1. American National Standards Institute (ANSI).
- B. Industry Standards:
 - 1. Department of Justice, Office of the Attorney General, "Americans with Disabilities Act", Public Law 101-336, (ADA).
 - 2. ANSI A117.1: Providing Accessibility and Usability for Physically Handicap People, 1986 edition.
 - 3. Federal Register Part III, Department of Justice, Office of the Attorney General, 28 CFR Part 36: Nondiscrimination on the Basis of Disability by Public Accommodations and in Commercial Facilities, Final Rule, July 26, 1991.
 - 4. ADA and ABA Accessibility Guidelines for Buildings and Facilities which was published in the Federal Register in July 2004.

1.3 DEFINITIONS

- A. Terms:
 - 1. Braille: Grade 2 Braille including 189 part-word or whole word contractions in addition to Grade 1 Braille 63 characters. Tactile is required whenever Braille is required; see SYSTEM DESCRIPTION Article below.
 - 2. Non-tactile: Letters and numbers on signs with width-to-height ratio between 3:5 and 1:1 and stroke width ratio between 1:5 and 1:10 using upper case "X" to calculate ratios. Use typestyles with medium weight; upper and lower case lettering is permitted; serif typestyles are permitted. See SYSTEM DESCRIPTION Article below.
 - 3. Symbols: Symbol itself is not required to be tactile but equivalent verbal description is required both in tactile letters and Braille.
 - 4. Tactile: 1/32" raised capital letters without serifs at least 5/8" height and not more than 2" height based on upper case "X". Braille is required whenever tactile is required; see SYSTEM DESCRIPTION Article below.

1.4 SYSTEM DESCRIPTION

- A. Signage under this section is intended to include items for identification, direction, control, and information of building where installed as complete integrated system from a single manufacturer.
- B. ADA design requirements:
 - 1. Signage requiring tactile graphics:
 - a. Wall mounted signs designating permanent rooms and spaces such as, room numbers and restroom, department, office, and fire exit identifications.
 - b. Individually applied characters are prohibited.
 - 2. Signage not requiring tactile graphics but require compliance to other ADA requirements: All other signs providing direction to or information about function of space such as, directional signs (signs with arrow), informational signs (operating hours, policies, etc.), regulatory signs (no smoking, do not enter), and ceiling and projected wall mount signs.
 - 3. Excluded signage:
 - a. Exterior signs.
 - b. Building directories.
 - c. Menus.
 - d. Temporary signs, include personnel signs and tenant identification; suite numbers are not considered temporary.
- C. ADA performance requirements:
 - 1. Tactile graphics signs mounting requirements:
 - a. Single doors: Mount 60 inches to sign centerline above finish floor and on wall adjacent to latch side of door.
 - b. Openings: Mount 60 inches to sign centerline above finish floor adjacent opening.
 - c. No wall space adjacent latch side of door, opening, or double doors: Mount 60 inches to sign centerline above finish floor on nearest adjacent wall.

1.5 SUBMITTALS

- A. Product Data: Provide the following information:
 - 1. Manufacturer's signed statement regarding compliance with QUALITY ASSURANCE Article.
 - 2. Manufacturer's product literature indicating units and designs selected.
 - 3. Evidence of manufacturer's computerized data retrieval program for tracking of Project for sign typography, message strip requirements and other pertinent data from schedule input to final computerized typography on finished product.
- B. Shop Drawings: Provide the following:
 - 1. Indicate materials, sizes, configurations, and applicable substrate mountings.
 - 2. Typography sample for message strips and headers copy.

3. Signage schedule complete with location of each sign and required copy; include floor plans.
- C. Samples: Full size samples for holder, insert, and copy in colors specified. Provide sample in small size sign. Samples will not be returned for use in Project.
- D. Contract Close Out: At Substantial Completion, provide the following:
1. Furnish appropriate checklist for aiding in reordering after Date of Substantial Completion. Maintain computer schedule program for five years for ordering new signage required by Government.
 2. Maintenance data and cleaning requirements for exterior surfaces.
 3. Furnish one complete software package Windows 3.0 or Windows 95 or later, Windows NT 4.0 or later in Government selected format for PC type computer.
 4. Furnish one complete packaged Color paper system with clear cover overlay.

1.6 QUALITY ASSURANCE

- A. Qualifications: Provide the following information for manufacturer:
1. Work required under this section from manufacturers regularly engaged in work of this magnitude and scope for minimum of five years.
 2. Maintain computer link between schedule input and computerized typography production.

1.7 DELIVERY, STORAGE, AND HANDLING

- A. Acceptance at site: Coordinate delivery of work to Project site under this section for immediate installation.

1.8 SEQUENCING AND SCHEDULING

- A. Schedule system installation after related finishes have been completed.

PART 2 - PRODUCTS

2.1 MANUFACTURED UNITS

- A. Design intent product is as follows. Sign system supplied by the contractor must be a manufacturer's supplied standard framed sign system that is equal to the following specification:
1. Refer to Drawing signage details. Signage to match UDC's standard interior signage for material, insert, color, and font type. Refer to image included in the specification.

2.2 FABRICATION

A. Shop assembly:

1. Fabricate units to configurations indicated on reviewed shop drawings. Internally reinforce units in accord with reviewed shop drawings.
2. Provide copy on inserts, message strips, headers or bases, and covers required on reviewed shop drawings and in accord with ADA requirements.
3. Wrap each individual unit with polyethylene.

PART 3 - EXECUTION

3.1 EXAMINATION

A. Verification of conditions: Indicated in Coordination Section.

1. Examine areas to receive signage; notify COR in writing of unacceptable substrate.
2. Beginning work indicates acceptance of substrate. Subsequent modifications to substrate or signage becomes this section's complete responsibility.

3.2 INSTALLATION

- A. Install signage holders in locations with mounting types indicated in accord with reviewed shop drawings. Square, plumb, and level units.
- B. Install inserts not more than 48 hours prior to Date of Substantial Completion complete with correct copy in place. Conform to ADA requirements for tactile graphics signage.

3.3 CLEANING

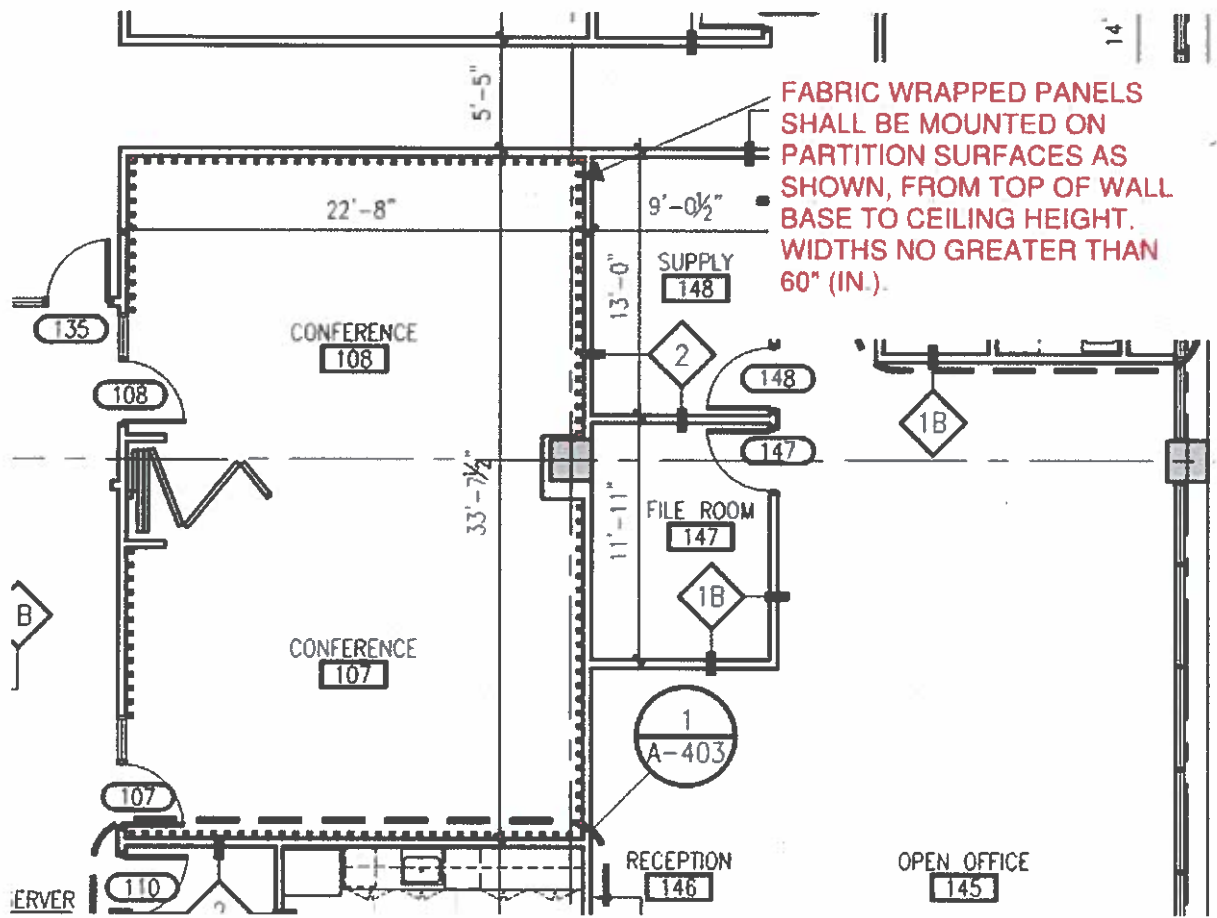
- A. Clean exposed surfaces not more than 48 hours prior to Date of Substantial Completion in accord with manufacturer's written cleaning instructions.

END OF SECTION 10443

C001

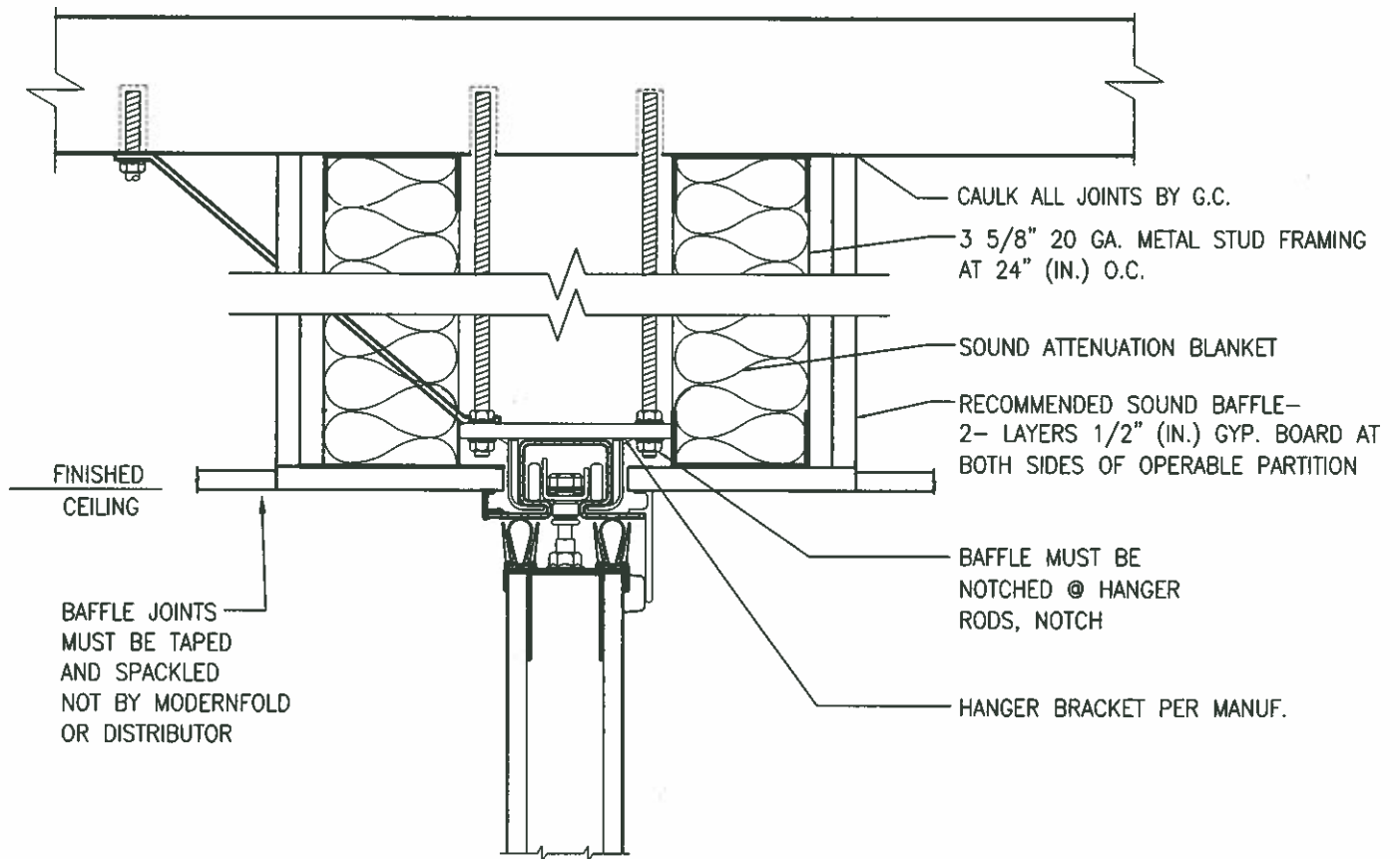
Technical Services

ATTACHMENT F



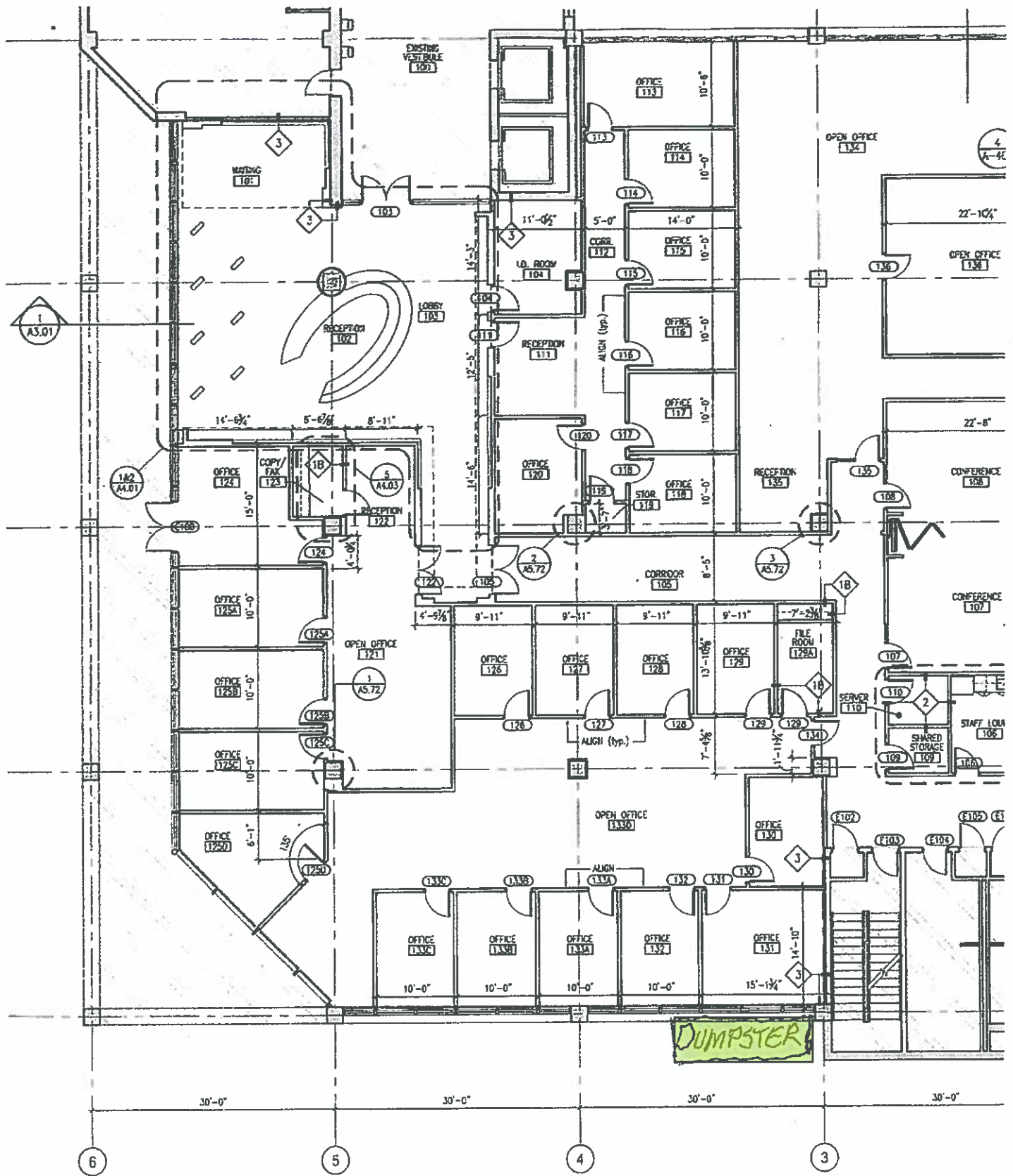
**BID QUESTION #5- FABRIC WRAPPED
 PANEL SKETCH**

ATTACHMENT G



**BID QUESTION #7- OPERABLE PARTITION
 SOUND BAFFLE SKETCH**

ATTACHMENT H



1 NEW WORK FLOOR PLAN - STUDENT SERVICES CENT
 A1.01 SCALE: 1/8" = 1'-0"
 LEVEL A ELEVATION: 21

BID QUESTION #11- DUMPSTER LOCATION

ATTACHMENT I

Clarification/ Supplemental Info #2- Access Panel Images



Large Access Panels



Small Access Covers

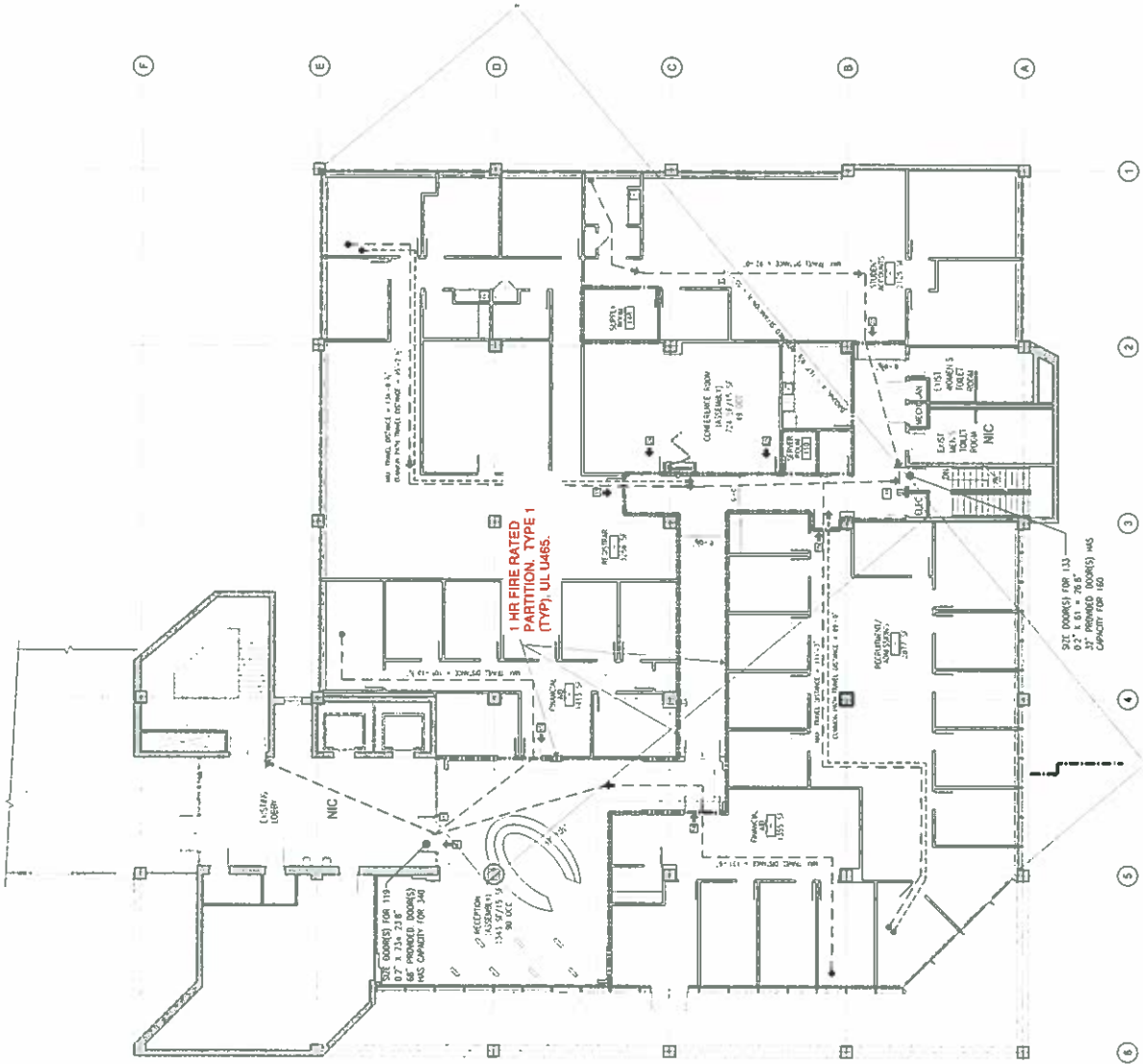
ATTACHMENT J

LEGEND



NOTES

- 1. ALL ROOMS SHALL BE PROVIDED WITH AN APPROVED (LISTED) FIRE DETECTOR.
- 2. COMMON AREAS SHALL BE PROVIDED WITH A MINIMUM OF ONE (1) EXITS TO THE OUTSIDE.
- 3. OCCUPANT LOADS SHALL BE BASED ON THE LATEST APPLICABLE CODE.



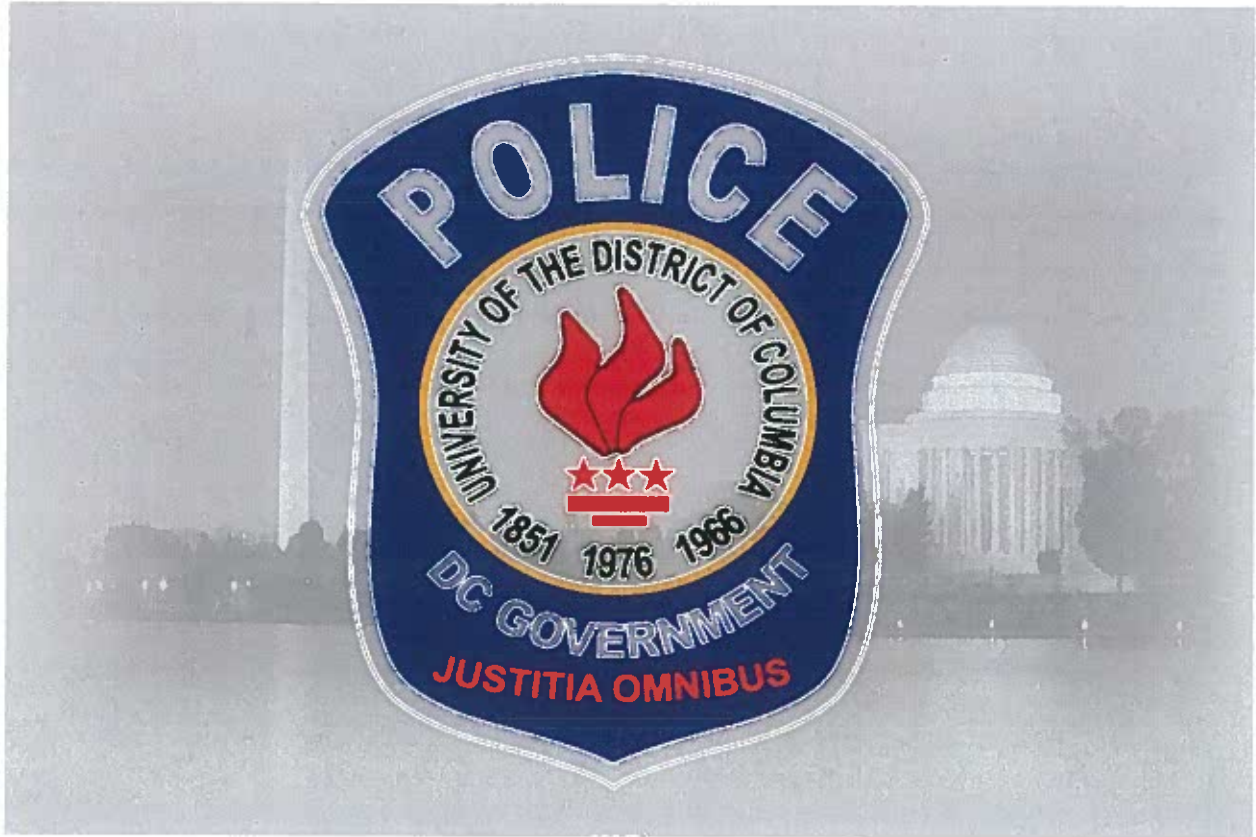
DATE	DESCRIPTION	DESIGNED BY	CHECKED BY	DATE
11/19/10	REV. ADMINISTRATION	11/19/10	11/19/10	11/19/10
11/19/10	REV. ADMINISTRATION	11/19/10	11/19/10	11/19/10
11/19/10	REV. ADMINISTRATION	11/19/10	11/19/10	11/19/10
11/19/10	REV. ADMINISTRATION	11/19/10	11/19/10	11/19/10
11/19/10	REV. ADMINISTRATION	11/19/10	11/19/10	11/19/10

PROJECT NO.	PROJECT NAME
13	GO.03
ARCHITECTURE	ARCHITECTURE
UNIVERSITY OF THE DISTRICT OF COLUMBIA	UNIVERSITY OF THE DISTRICT OF COLUMBIA
STUDENT SERVICES CENTER	STUDENT SERVICES CENTER
LEVEL A ELEVATION 200.0'	LEVEL A ELEVATION 200.0'
DATE	DATE
11/17/2011	11/17/2011

LIFE SAFETY PLAN - STUDENT SERVICES CENTER
LEVEL A ELEVATION 200.0'

Clarification/ Supplemental Info #4 - Corridor Fire Rating
For Reference Only - Not for Construction

ATTACHMENT K



OFFICE OF PUBLIC SAFETY/POLICE
University of the District of Columbia
Integrated Security Management
Specifications

12.1.2011

The University is responsible and accountable to ensure the safety and well being of the academic community. Crime is a serious problem that faces all colleges and universities today. The types of crime educational institutions experience range from trespassing, burglary and theft to physical and sexual assault, and armed robbery.

The University is an educational institution whose primary mission, to educate, in safe and secure academic buildings. These buildings house the activities which require the faculty, students, and staff to assemble. Many academic buildings are multi-use buildings that operate twenty-four hours per day, seven days a week. The more academic programs and activities a facility generates, the larger the responsibility it is to provide adequate safety and security measures to protect both people and property. Security measures may vary based on the facility size and the level of activities.

This security measures in this standard provides building protection to typical multi-use academic buildings at the University of the District of Columbia. The standard has been developed by utilizing years of experience, recognizing the diverse needs, and collecting acceptable ideas and practices that have proven to increase security and safety.

The standard utilizes (CPTED) Crime Prevention Through Environmental Design concepts, which expand on the assumption that proper design and effective use of the built environment, can lead to a reduction in the fear of crime and incidence of crime, and to an improvement in the quality of life. Standards may require architectural, electronic, and operational measures.

The intent of an established standard is to provide a balance and consistent approach for security methods and measures across the campus. Standards do not eliminate the need for knowledge and judgment. Standards present solutions that are valid for most conditions, but in certain demanding cases more stringent provisions may be justified with the Office of Public Safety's approval. Similarly, conditions may exist which permit less extensive alternate solutions.

Multipurpose buildings house classrooms, lecture halls, libraries, laboratories, research facilities, shops, cafeterias, faculty and administrative offices student centers, etc. The perimeters of the buildings have pedestrian entrances, emergency exits, receiving docks, windows, and utility openings that require protection from unauthorized or illegal entry. This is a challenge since the buildings are heavily populated and are extremely active around the clock.

Pedestrian Entrances

All buildings have recognizable-designated pedestrian entrances. It is recommended to minimize the amount of entrances to channel pedestrian traffic to support the access control management. All pedestrian entrances are recognized as authorized building exits. All entrances shall be provided with the following security measures:

- All entry doors, frames, window panes, and locks on the building's perimeter must be resistant to forcible entry. The doors must be able to close and lock from the outside and provide emergency egress from the inside.

- Entrance doors must be equipped with the campus standard access control card readers, electric locks, and intrusion propped door sensors.

The access control system is a computer security management system that grants authorized cardholder's access to the protected areas during predetermined programmable time periods. It maintains a transaction record of all entries to the building. Multipurpose buildings are open during normal operating hours and closed and locked after hours. After normal operating hours, all faculty, students, and staff with predetermined authorized privileges may use their UDC ONEcard as a key to enter the locked buildings. Through the access control system's programming, lost, stolen, and expired cards can be deactivated which denies access to protected buildings and other areas. The Office of Public Safety centrally monitors the access control system 24-hours per day.

- All entry doors must be equipped with intrusion/propped door alarm sensors. The Intrusion propped door sensors monitor the open/closed position of the door. The sensor will detect a door that is forced open or if a door is illicitly propped open.
- All electric lock and door conditions must be inspected and tested for proper operation quarterly. Preventive maintenance must be performed on the doors every six months.
- All intrusion/propped door alarms must be inspected and tested for proper operation every six months.

Emergency Exits

All buildings are equipped with exit doors used for pedestrian egress in case of an emergency. The numbers of emergency exits are based on life safety requirements, the architectural make up of the building, and the population the building exit is designed to accommodate. All emergency exits must be provided with the following security measures:

- All entry doors, frames, window panes, and locks on the building's perimeter must be resistant to forcible entry. The doors must be able to close and lock from the outside and provide emergency egress from the inside.
- All entry doors must be equipped with intrusion door alarm sensors. The sensor will detect a door that is forced open.
- All intrusion/propped door alarms must be inspected and tested for proper operation every six months.

Receiving Docks

The receiving docks are considered entrances. All receiving dock entrances must be provided with the same security measures as an entrance door.

Windows

Most buildings are equipped with air conditioning, but many buildings have operable windows for fresh air ventilation.

- All building operable windows must be closed and locked when not used for ventilation. All building occupants are responsible to ensure windows are properly secured after normal operating hours. The Office of Public Safety will periodically patrol and inspect the buildings perimeter for unsecured windows.
- All accessible windows less than 14' from ground level or adjacent to buildings, fire escapes, rooftops, etc. must be equipped with window security barriers such as burglar resistant window screens or perforated metal.

Building Utility and Rooftop Openings

Many buildings have accessible utility and rooftop opens that an intruder can gain access to the buildings.

- Any utility opening that is greater than 10 inches square that an intruder could enter and exit the building must have an effective security barrier such as bars, grills, or operable gates.
- All accessible utility and rooftop passages such as grills, gates, hatches, utility doors, etc. must be equipped with appropriate intrusion alarm sensors.

UDC INTEGRATED SECURITY MANAGEMENT SYSTEM

PART 1 — GENERAL

SUMMARY: The intent of this document is to specify the minimum criteria for the supply, installation, integration and activation of Satellite/Branch campus security management system (SMS) with UDC's Main Campus SMS. The Main campus SMS is on the Honeywell ProWatch platform. **All work must be coordinated and approved through UDC Police, Technology Services Division and Advantech, Inc. (UDC's existing security systems integrator). All work must be supplied, installed, and programmed by a Honeywell ProWatch Platinum Certified Systems Integrator (certification with the Honeywell Software Design Kit) as well as be a Salto Trained Inspired Business Partner (TIBP). Security integrator must have documented experience working in a security environment that has an integrated ProWatch/Salto System.**

1.1 REFERENCES

- A. Reference Standards: Systems specified in this Section shall meet or exceed the requirements of the following:
1. Federal Communications Commission (FCC):
 - a. FCC Part 15 – Radio Frequency Device
 - b. FCC Part 68 – Connection of Terminal Equipment to the Telephone Network
 2. Underwriters Laboratories (UL):
 - a. UL294 – Access Control System Units
 - b. UL1076 – Proprietary Burglar Alarm Units and Systems
 3. National Fire Protection Association (NFPA):
 - a. NFPA70 – National Electrical Code
 4. Electronic Industries Alliance (EIA):
 - a. RS232C – Interface between Data Terminal Equipment and Data Communications Equipment Employing Serial Binary Data Interchange
 - b. RS485 – Electrical Characteristics of Generators and Receivers for use in Balanced Digital Multi-Point Systems
 5. Federal Information Processing Standards (FIPS):
 - a. Advanced Encryption Standard (AES) (FIPS 197)
 - b. FIPS 201: Personal Identity Verification (PIV) of Federal Employees and Contractors
 6. Homeland Security Presidential Directive 12 (HSPD-12)

1.2 SECURITY MANAGEMENT SYSTEM DESCRIPTION

- A. The Security Management System shall function as an electronic access control system and shall integrate alarm monitoring, CCTV, digital video, ID badging and database management into a single platform. A modular and network-enabled architecture shall allow maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.

1.3 SUBMITTALS

- A. **Manufacturer's Product Data:** Submit manufacturer's data sheets indicating systems and components proposed for use.
- B. **Shop Drawings:** Submit complete shop drawings indicating system components, wiring diagrams and load calculations.
- C. **Record Drawings:** During construction maintain record drawings indicating location of equipment and wiring. Submit an electronic version of record drawings for the Security Management System not later than Substantial Completion of the project.
- D. **Operation and Maintenance Data:** Submit manufacturer's operation and maintenance data, customized to the Security Management System installed. Include system and operator manuals.
- E. **Maintenance Service Agreement:** Submit a sample copy of the manufacturer's maintenance service agreement, including cost and services for a two year period for Owner's review.

1.4 QUALITY ASSURANCE

- A. **Manufacturer:** Minimum ten years' experience in manufacturing and maintaining Security Management Systems. Manufacturer shall be Microsoft Gold Certified.
- B. **Installer and Security Integrator** must be **Platinum** certified by Honeywell Integrated Security Dealer Service Certification Program (DSCP). Platinum certification ensures that the Installed

and Security Integrator is Integration Capable and has met the highest standards of technical competence and customer service.

- C. Installer and Security Integrator must be PROWATCH Security Management System (SMS) certified by Honeywell Integrated Security. Certification must be evidenced by the full time employment of multiple PROWATCH SMS certified (successful completion of manufacturer training) technicians and must also be certified in the Honeywell Software Development Kit (HSDK).
- D. Installer and Security Integrator must be MaxPro Video Management System (PROWATCH Video Manager) certified by Honeywell Integrated Security. Certification must be evidenced by the full time employment of multiple MaxPro VMS certified (successful completion of manufacturer training) technicians.
- E. Installer and Security Integrator must be Enterprise certified by Honeywell Integrated Security. Certification must be evidenced by the full time employment of multiple MaxPro VMS certified (successful completion of manufacturer training) technicians.
- F. Installer and Security Integrator must be a Salto Trained Inspired Business Partner (TIBP). TIBP must be evidenced by the full time employment of multiple Salto certified (successful completion of manufacturer training) technicians.

G. Installer and Security Integrator must also show evidence by the full time employment with Prowatch & Salto working seamlessly in an integrated environment (same as in the University of the District of Columbia).

1.5 DELIVERY, STORAGE, AND HANDLING

- A. Deliver materials in manufacturer's labeled packages. Store and handle in accordance with manufacturer's requirements.

1.6 WARRANTY

- A. Manufacturer's Warranty: Submit manufacturer's standard warranty for the security management system.

PART 2 – PRODUCTS

2.1 INTEGRATION REQUIREMENTS FOR VAN NESS AND SATELLITE/BRANCH CAMPUSES

- A. The Security Management System, herein referred to as System or SMS, and the Sub-systems shall be modular and networkable. The System shall be controlled by UDC's existing

Honeywell PROWATCH Version 3.8 software. All work shall be coordinated and approved through UDC Police, Technology Services Division and **Advantech, Inc.** (UDC's existing Security Systems Integrator). All work must be supplied, installed and programmed by a **Honeywell Integrated Security Platinum Certified Systems Integrator**. This System Integrator must also be certified and manufacturer trained for the following: Salto Virtual Networked Access Control Locks, Honeywell PROWATCH SMS, Honeywell MaxPro VMS, and Honeywell Enterprise integrated as one system.

UDC's existing Security Systems Integrator is ADVANTECH, Inc. Telephone: 877-674-8405, Email: daves@advantechsecurity.net or eric@advantechsecurity.net

- B. Any required Security Workstations, Servers, Storage Arrays, Laptops, Touchscreens, Network Switches, Racks/Enclosures and UPSs indicated in the drawings or specifications for this project must be pre-approved by UDC's existing Security Systems Integrator. Pre-approval must be evidenced by a compliance document listing the required technical specifications of each item.

2.2 MANUFACTURER

- A. Security Management System Manufacturer: Pro-Watch® Security Management Suite by Honeywell, www.honeywellintegrated.com. Provide the following software system:
 - 1. Pro-Watch® Corporate Edition.

2.3 SECURITY MANAGEMENT SYSTEM SOFTWARE REQUIREMENTS

Software Requirements: The Security Management System shall be a modular and network-enabled access control system. The Security Management System shall be capable of controlling multiple remote sites, alarm monitoring, video imaging, ID badging, paging, digital video and CCTV switching and control that allows for easy expansion or modification of inputs and remote control stations. The Security Management System control at a central computer location shall be under the control of a single software program and shall provide full integration of all components. It shall be alterable at any time depending upon facility requirements. Security Management System reconfiguration shall be accomplished online through system programming. **THE ADDITIONAL CARD READER LICENSES, CAMERA LICENSES, ADDITIONAL PROWATCH CE CLIENT LISENCE AND ADDITIONAL MAXPRO VMS CLIENT LICENSES SHALL BE PROVIDED AS A PART OF THIS PROJECT. IN ADDITION THE MANUFACTURER'S SSA (SOFTWARE SUPPORT AGREEMENT) FOR ALL PROWATCH LICENSES AND SUB-SYSTEM LICENSES SHALL BE INCLUDED FOR THE FIRST YEAR OF SYSTEM OPERATION. ALL REQUIRED PROGRAMMING OR LICENSING SHALL BE COORDINATED THROUGH AND PROVIDED BY UDC'S EXISTING SECURITY SYSTEMS INTEGRATOR.**

- A. The Security Management System shall include the following:

1. **Multi-User/Network Capabilities:** The Security Management System shall support multiple operator workstations via local area network/wide area network (LAN/WAN). The communications between the workstations and the server computer shall utilize the TCP/IP standard over industry standard IEEE 802.3 (Ethernet). The communications between the server and workstations shall be supervised, and shall automatically generate alarm messages when the server is unable to communicate with a workstation. The operators on the network server shall have the capability to log on to workstations and remotely configure devices for the workstation. Standard operator permission levels shall be enforced, with full operator audit.
2. **Concurrent Licensing:** The Security Management System shall support concurrent client workstation licensing. The Security Management System application shall be installed on any number of client workstations, and shall provide the ability for any of the client workstations to connect to the database server as long as the maximum number of concurrent connections purchased has not been exceeded.
3. **Security Key:** The Security Management System shall only require a single security key dongle to be present on the database server for the Security Management System to operate. Security keys shall not be required at the client workstations. The Security Management System shall allow a user to read the information that is programmed on the server security key dongle. The Security Management System shall support export of the information using the 'Export Dongle information' button, which shall allow the user to forward to the integrator when upgrading new dongle features.
4. **Access Control Software Suite:** The Security Management System shall offer a security management software suite available in four scalable versions: Lite, Professional, Corporate, and Enterprise Editions. The Security Management System platform shall offer a complete access control solution: alarm monitoring, video imaging, ID badging and video surveillance control.
 - a. **Corporate Edition:** The Security Management System shall operate in the Windows Server 2003 (32-bit) or Windows Server 2008 (32-bit and 64-bit) environment and utilize SQL 2005 (32-bit) or SQL 2008 (32-bit or 64-bit) as the database engine.
5. **Terminal Services:** The Security Management System shall support Windows Server 2003/2008 Terminal Services. Terminal Services shall allow the Security Management System server application to reside on the Windows Terminal Server. Operating systems supporting a standard web browser shall be capable of utilizing the thin client architecture. The Security Management System shall support unlimited connections, based on concurrent licensing, to the Security Management System software. Full

functionality shall be obtained through the intranet connection allowing full administration and monitoring without the need for a local installation.

6. **Relational Database Management System:** The Security Management System shall support industry standard relational database management systems. This shall include relational database management system Microsoft SQL Server 2005/2008.
7. **Database Partitioning:** The Security Management System shall provide the option to restrict access to sensitive information by user ID.
8. **Memory:** Proprietary software programs and control logic information used to coordinate and drive system hardware shall be stored in read-only memory.
9. **LDAP/ Microsoft Active Directory Services:** The Security Management System shall provide support of Lightweight Directory Access Protocol (LDAP) for enabling the user to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public internet or on a private intranet. The Security Management System shall provide a direct link to Microsoft Active Directory Services. The Security Management System shall allow the transfer of Active Directory users into the database via the Data Transfer Utility. Conversely, Security Management System users shall be capable of being exported to the Active Directory.
10. **Unicode:** The Security Management System shall utilize Unicode worldwide character set standard. The Security Management System shall support double-byte character sets to facilitate adaptation of the Security Management System user interface and documentation to new international markets. Language support shall include at a minimum English, Spanish, Portuguese, French, German and Simple Chinese.
11. **Encryption:** The Security Management System shall provide multiple levels of data encryption
 - a. True 128-bit AES data encryption between the host and intelligent controllers. The encryption shall ensure data integrity that is compliant with the requirements of FIPS-197 and SCIF environments. Master keys shall be downloaded to the intelligent controller, which shall then be authenticated through the Security Management System based on a successful match.
 - b. Transparent database encryption, including log files and backups

- c. SQL secure connections via SSL

- 12. Supervised Alarm Points: Both supervised and non-supervised alarm point monitoring shall be provided. Upon recognition of an alarm, the system shall be capable of switching CCTV cameras that are associated with the alarm point.

- 13. Compliance and Validation: The Security Management System shall incorporate signature authentication where modifications to Security Management System resources will require either a single or dual signature authentication. Administrators will have the ability to select specified devices in the Security Management System where data manipulation will be audited and signatures will be required to account for the data modification. Upon resource modification, the user will be required to enter a reason for change or select a predefined reason from a list. All data will be securely stored and maintained in the database and can be viewed using the reporting tool. This functionality will meet the general requirements of Validation and Compliance through Digital Signatures with special attention to the case of Title 21 CFR Part 11 Part B compliance.

- 14. Clean Room Solution:
 - a. Overview: The Security Management System shall provide a clean room solution which enables users to manage their "Clean Environments" or other areas requiring special restricted access through a process-oriented graphical user interface (GUI).
 - b. Configuration: The user shall have the capability of adding, editing, or deleting clean rooms. Each "clean room" shall be capable of having a contamination level set. Entry to a higher level contamination area shall automatically restrict access to cleaner level areas. Individual cards shall be capable of being reset on an immediate one time, automatic, or per-hour basis.

2.4 OPERATIONAL REQUIREMENTS

A. Security Management System Operational Requirements:

1. System Operations:

- a. Password: The Security Management System shall use an integrated authentication method which utilizes Windows user accounts and policies.

- b. Information Access: The Security Management System shall be capable of limiting operator access to sensitive information. Operators must have proper authorization to edit the information.
- c. Shadow Login: The Security Management System shall allow users to login over a currently logged-on user without having the current user log off the Security Management System or out of the Windows operating system.
- d. Graphical User Interface: The Security Management System shall be fully compliant with Microsoft graphical user interface standards, with the look and feel of the software being that of a standard Windows application, including hardware tree-based system configuration.
- e. Help: The main Security Management System user interface shall include a help icon which shall require only one click to activate. The standard special function key "F1" shall have the capability to be programmed to provide access to the help system.
- f. Guard Tour: The Security Management System shall include a guard tour module, which shall allow the users to program guard tours for their facility. The tours shall not require the need for independent or dedicated readers.
- g. Secure Mode Verification (e.g., force guard to do a visual verify): The Security Management System shall provide 'secure mode' control from the verification viewer. This shall allow a user or guard to decide the access of an individual who presents his/her card at a designated secure mode reader.
- h. Database Partitioning: The Security Management System shall support dynamic partitioning. A Security Management System in which partitions are set up at installation and cannot be easily changed shall not be acceptable.
- i. Status Groups: The Security Management System shall support a real-time system status monitor that graphically depicts all logical devices.

- j. **Keyboard Accelerators:** The Security Management System shall allow the user to use a shortcut key to enable designated system commands.
- k. **Automatically Disable Card upon Lack of Use:** The Security Management System shall allow system operators to set a predefined time period in which cardholders must swipe their card through a card reader in the Security Management System.
- l. **User Functions and ADA Ability:** The Security Management System shall provide user functions and ADA (Americans with Disabilities Act) ability that provides the capability to trigger an event at the Security Management System intelligent controller when a defined card is presented.
- m. **Pathways:** The Security Management System shall support the capability of programming pathways. A pathway shall be an object that combines input points to be masked (shunted) for a set duration, and an output point to be activated, when a particular card receives a local grant at a reader.
- n. **Database Audit Log:** The Security Management System shall be capable of creating an audit log in the history file following any change made to the Security Management System database by an operator.
- o. **Operator Log:** The Security Management System shall be capable of creating an action log in the history file following actions performed by an operator.
- p. **Alarm Routing:** The Security Management System shall be capable of defining routing groups that determine what event information shall be routed to a user or class of users.
- q. **Global and Nested Anti-passback:** The Security Management System shall support the use of an optional anti-passback mode, in which cardholders are required to follow a proper in/out sequence within the assigned area.
- r. **Two Person Rule:** The Security Management System shall support a “two person rule” to restrict access to specific access areas unless two cardholders present two

different valid cards to the reader one after the other within a period time defined by the door unlock time multiplied by a factor of 2.

- s. **Occupancy Restrictions:** The Security Management System shall allow the user to define the minimum and maximum occupancy allowed in a designated area.
 - t. **Multiple Sequential Card Swipes to Initiate Procedure:** The Security Management System shall allow the user to define a logical device, quantity of consecutive identical events, a time period and a Security Management System procedure to trigger when the event occurs that quantity of times in the allocated time period.
 - u. **Hardware Templates:** The Security Management System shall include the ability to define hardware templates (door templates) in order to simplify the process of creating an access control system. Hardware templates shall allow a user to define a "typical" door configuration and then use that template over and over in the process of defining doors.
2. **Access Control Functional Requirements:** Functions shall include validation based on time of day, day of week, holiday scheduling, site code verification, automatic or manual retrieval of cardholder photographs, and access validation based on positive verification of card/PIN, card, and video. The following features shall be programmable and shall be capable of being modified by a user with the proper authorization:
- a. **Time Zones:** Shall define the period during which a reader, card, alarm point, door, or other system feature is active or inactive. In addition to Monday-Sunday, there shall be at least one day of the week called Holiday.
 - b. **Holidays:** The application shall allow holidays to be entered into the Security Management System. Holidays shall have a start date plus duration defining multiple days. Holidays shall have a holiday type of 1, 2, or 3, which may be defined by the user.
 - c. **Response Codes:** The Security Management System shall allow the user to enter a predefined code to represent a response to an alarm occurring in the facility.

- d. Clearance Codes: The Security Management System shall allow the user to establish groups of readers at a facility for the purpose of granting or denying access to badgeholders. Clearance codes shall be assigned to companies and individuals employed by the company, and may be modified for individual users in the badgeholder maintenance application.
- e. Companies: Each badgeholder entered into the Security Management System shall be assigned a company code identifying the individual's employer. The company information dialog box displays and maintains information related to companies having access to the facility.
- f. Group Access: The Security Management System shall allow a user or group of users via company selection, a temporary denial of access to specific readers or areas based on a preconfigured event. The group access function shall limit access to a group of cardholders, overriding all other access criteria.
- g. Events: The event editors shall control processing done at the host computer that allows the user to associate nearly any input (trigger) with almost any sequence of outputs (actions) that the Security Management System is capable of executing.
- h. Alarm Pages: Security Management System shall include the capability to create an unlimited number of customized alarm pages for the alarm monitor and each shall be assignable to users and user classes.
- i. Event Types: Definitions shall be shipped with system software but shall be capable, upon installation, of being modified, added to, or deleted from the Security Management System.
- j. Dynamic Graphical Maps: The Security Management System shall provide the user with the means to add maps and indicator icons to maps that shall represent input/output points, logical devices, or cameras located throughout the Security Management System. Security Management System maps shall display the state and condition of alarm points. The Security Management System shall also provide the ability to monitor the channels or panels.
- k. Brass Keys: Shall maintain information related to assets that are issued in the facility, including brass keys, laptops, RSA keys, cell phones, company cards, etc.

- I. ID Badging Client: The Security Management System Shall maintain information related to a badgeholder's card access privileges. Upon entering this application, a window shall appear on the screen and all actions (add, modify, or delete) involving badges and cards shall be initiated from this window. Access privileges shall be linked to the cards used to gain access to doors in the facility. Modifications shall be made by adding or deleting clearance codes, or by door types assigned to the cards or to a badgeholder.

- m. ID Badging System: The Security Management System shall include seamlessly integrated ID badging system.

- n. Users: Information related to the users of the Security Management System software shall be stored in the database. Users entered into the Security Management System shall be assigned the access privileges of the class to which they are assigned.

- o. Elevator Control: The elevator control shall be of the Security Management System intelligent controller-based line of devices. The elevator control shall include the following functional features:
 - 1) Elevator call: Valid card read calls elevator to the floor. No reader in the elevator car.

 - 2) Floor control: Valid card read in the elevator car enables selectable floor buttons.

 - 3) Floor select: Valid card read in the elevator car enables selectable floor buttons and logs which floor is selected after the card is presented.

- p. Data Transfer Unit (DTU): The DTU enables data to be transferred from and external system directly into the Security Management System database.
 - 1) Insert only: If a "data file key column #" shall be provided, the DTU will only insert a new badge record if the key column value is not found. An error shall

be displayed in the log file if an existing badge record is found. If no "data file key column #" is provided, every record will be inserted into the Security Management System.

- 2) Updates only: The DTU shall use the "data file key column #" to look for the matching Security Management System record. An error shall be logged in the log file if the badgeholder is not found in the Security Management System database.
 - 3) Inserts, updates: The DTU shall use the "data file key column #" to look for the matching Security Management System record. If a matching record is not found, the DTU shall insert the data. If a matching record is found, the record shall be updated.
- q. Generic Channel Interface: The Security Management System shall provide the ability to define generic communications channels over serial port or TCP/IP network socket including IP address and port/socket, to support custom integration of external foreign devices. The Security Management System shall generate events based on data received from the channel matching operator pre-defined instructions.
3. Application Localization: The Security Management System shall support at least seven languages including English. The languages available must include German, French, Spanish, Italian, Chinese (simplified), Portuguese (Brazil), Norwegian, Chinese (Traditional), Danish, and Dutch. All database resources will be localized, and will include a standard U.S. English help file.
 4. Event Manager: The Security Management System shall utilize an event manager as a component of system administration and offer the ability to have users control the amount of data stored as well as a quick snapshot of the logged data in the system. Using the various logs in event manager, the user will be able to gather information about events, auditing, and operator actions. The logs are defined as follows: Event log, audit log, unacknowledged alarms.

2.5 HARDWARE REQUIREMENTS

A. INTELLIGENT CONTROLLERS

1. Distributed architecture shall allow controllers to operate independently of the host. The architecture shall place key access decisions, event/action processing and alarm monitoring functions within the controllers, eliminating degraded mode operation.
2. Flash memory management shall support firmware updates and revisions to be downloaded to the system. Upgrades to the hardware and software shall occur seamlessly without the loss of database, configurations, or historical report data.
3. Manufacturers: Subject to compliance with requirements, provide Field Controllers or comparable product by one of the following:
 - a. Honeywell Security Star I
 - b. Honeywell Security Star II
 - c. Honeywell Security PW-2000
 - d. Honeywell Security PW-5000
 - e. Honeywell Security PW-6000
4. Cardkey Controllers: The Security Management System software suite shall provide functionality to Cardkey Controllers using Nodal Protocol B, the Cardkey Controllers D620 (Firmware revision PS-143D or PS143-E), and the Cardkey D600AP (Firmware Revisions PS-155A or PS-155B). Supported interface is currently, but not limited to, standard STI and STIE devices. Minimum functionality to be supported:
 - a. Controller to host communications.
 - b. Downloading of cards.
 - c. Downloading of Security Management System parameters.
 - d. Downloading of reader parameters.
 - e. Downloading of input point parameters.
 - f. Downloading of relay output point parameters.

B. FIELD HARDWARE

1. The security management system shall be equipped with access control field hardware required to receive alarms and administer all access granted/denied decisions. All field hardware shall meet UL requirements.
2. Intelligent Controller Board
 - a. Honeywell Security PW3K1IC
 - b. Honeywell Security PW6K1IC
3. Dual Reader Module (DRM)
 - a. Honeywell Security PW6K1R2
4. Alarm Input Module (AIM)
 - a. Honeywell Security PW6K1IN
5. Relay Output Module (ROM)
 - a. Honeywell Security PW6K1OUT
6. Card Readers
 - a. HID
 - 1) iClass R40, 13.56MHz Smart Card Reader, Single-gang Mount
 - 2) iClass R15, 13.56MHz Smart Card Reader, Mullion Mount
 - b. Biometric Readers
 - 1) BioScript
 - 2) Recognition Systems
 - 3) MorphoTrak

2.6 SYSTEM INTERFACES

A. Digital Video Recording Systems

1. The Security Management System shall provide fully integrated support for a powerful digital video recording and transmission system. The Security Management System shall record, search and transmit video, and shall provide users with live, pre- and post- event assessment capabilities. The DVRs shall be seamlessly integrated with existing video equipment and incorporated into any TCP/IP network. The DVRs shall provide multiple levels of integration with the Security Management System software, providing control of the digital video system from the access control application.
2. Manufacturer(s) and part numbers:
 - a. Honeywell MAXPRO® VMS with PROWATCH Connector (PROWATCH VIDEO MANAGER)
 - b. Honeywell Enterprise Network Video Recorders. Sized to provide 30 days of video storage @ RAID5 for the project designated number of cameras, with a recorded resolution of 1280x720 at 5 ips. Provide multiple recorders if necessary. All recorders to be provided with rack-mount UPS in accordance with the UDC Public Safety requirements.

B. Video Management Systems (VMS):

1. With integration to VMS, Security Management System shall control multiple sources of video subsystems in a facility to collect, manage and present video in a clear and concise manner. VMS intelligently determines the capabilities of each subsystem across various sites, allowing video management of any analog or digital video device through a unified configuration and viewer. Disparate video systems are normalized and funneled through a common video experience. Drag and drop cameras from the Security Management System hardware tree into VMS views. Leverage Security Management System alarm integration and advanced features such as pursuit that help the operator track a target through a set of sequential cameras with a single click to select a new central camera and surrounding camera views.
2. Manufacturer(s) and part numbers:
 - a. Honeywell Security MAXPRO VMS

C. Cameras:

1. Indoor/Outdoor Fixed Position: Honeywell HD4MDIP 720p High Definition IP Camera, Day/Night, Impact Resistant. Include appropriate mount for the application.

2. Indoor Fixed Position: Honeywell HD3MDIP 720p High Definition IP Camera, Day/Night. Include appropriate mount for the application.
3. Pan, Tilt, Zoom Outdoor: Honeywell HDXGNWDCW PTZ IP Camera, Day/Night, Wide Dynamic Range, 35x Zoom, Image Stabilization. Include appropriate mount and power supply for the application.
4. Pan, Tilt, Zoom Indoor: Honeywell HDXGNPDCW PTZ IP Camera, Day/Night, Wide Dynamic Range, 35x Zoom. Include appropriate mount and power supply for the application.

D. Virtual Network Wireless Electronic Access Control Locksets:

1. Salto ANSI Mortise Lockset with iClass card reader, Privacy Button, Wireless Ready.
2. Salto Cylindrical Lockset with iClass card reader, Privacy Button, Wireless Ready.
3. Salto Hot Spot Reader/Encoder.

E. Intercom Interface:

1. The interface shall provide control of both remote and master intercom stations from within the Security Management System application. The Security Management System shall allow the user to define the site, channel, description, and address as well as provide a checkbox for primary station.
2. Administrators shall have the capability to program a list of intercom functions that report to the alarm-monitoring module as events. These functions shall coincide with the intercom functions provided with the intercom system. For each intercom function, Security Management System administrators shall be able to define an alphanumeric event description 1 to 40 characters in length and shall also be able to set the parameter value of that function.
3. The intercom interface shall allow for secondary annunciation of intercom calls, events, and alarms in the alarm-monitoring window. Intercom reporting to the alarm monitoring

window shall report as any other access control alarm and shall have the same annunciation and display properties as access control alarms.

4. All intercom calls, events, and alarms that report into the Security Management System shall be stored in the system database for future audit trail and reporting capabilities. Intercom events shall include but not be limited to: Station busy, Station free, Intercom call to busy station, Intercom call to private station, Station disconnected, Function dialed outside connection, Intelligent station ID, Station reset, Station lamp test, Audio program changed, Group hunt occurred, Mail message, Digit dialed during connection, Direct access key pressed, Handset off hook, M-key pressed, C-key pressed
5. Manufacturer(s) and part numbers:
 - a. Stentofon/Zenitel Alphacom series intercoms
 - b. Commend series intercoms

F. Intrusion Detection Panels:

1. Honeywell VISTA-128FBP and VISTA-250FBP Controllers:
 - a. General Requirements: The Security Management System shall support hardwired and TCP/IP communication for the VISTA 128FBP/VISTA-250 FBP panel. Each panel shall have 8 partitions and 15 zone lists. Zones, partitions, and the top-level panel shall have an events page, with all supported events present. Features:
 - 1) Disarm and unlock a door on card swipe.
 - 2) Arm and lock a door on card swipe.
 - 3) Common area arm/disarm.
 - 4) Access denied if intrusion system is in alarm or armed.
 - 5) Monitor and log intrusion system events and alarms in the Security Management System.
 - 6) Associate intrusion system events and alarms to video surveillance integrations.

2. Honeywell Galaxy Dimension GD264 and GD520 Controllers:
 - a. Security Management System users are able to control and monitor Group and zone status using the Security Management System client, and control the individual zones and groups using Security Management System Access control credentials. Depending on the combined user profiles and access permissions defined in Security Management System, a Security Management System cardholder is allowed or denied permission to arm/disarm zones and groups. The access control functionality of the intrusion panel is disabled when the integration is operational. Features:
 - 1) Disarm a zone on a card swipe.
 - 2) Arm a zone on consecutive card swipes. Security Management System will support definition of quantity of swipes required and the timeout time in seconds to recognize consecutive swipes.
 - 3) Security Management System supports linking of intrusion panel users with Security Management System cardholders.
 - 4) Security Management System operators may be given control permissions for intrusion input and output alarms.
 - 5) Security Management System can associate alarm events with video commands to look at current or historic footage.
 - 6) Security Management System stores and reports on intrusion events.

G. Software Development Kit (SDK)

1. Security Management System shall permit custom integration with other third party systems through an SDK. SDK shall support the OBIX communication protocol and interface directly with the Niagara Framework for support of additional communications protocols.
2. Manufacturer(s) and part numbers:
 - a. Honeywell Security HSDK

PART 3 — EXECUTION

3.1 EXAMINATION

- A. Examine site conditions to determine site conditions are acceptable without qualifications. Notify Owner in writing if deficiencies are found. Starting work is evidence that site conditions are acceptable.

3.2 INSTALLATION

- A. Security Management System, including but not limited to access control, alarm monitoring, CCTV and ID badging system shall be installed in accordance with the manufacturer's installation instructions.

- B. Supervise installation to appraise ongoing progress of other trades and contracts, make allowances for all ongoing work, and coordinate the requirements of the installation of the Security Management System.

3.3 FIELD TESTING AND CERTIFICATION

- A. Testing: The access control, alarm monitoring, CCTV, and ID badging system shall be tested in accordance with the following:
 - 1. Conduct a complete inspection and test of all installed access control and security monitoring equipment. This includes testing and verifying connection to equipment of other divisions such as life safety and elevators.
 - 2. Provide staff to test all devices and all operational features of the Security Management System for witness by the Owner's representative and authorities having jurisdiction as applicable.
 - 3. Correct deficiencies until satisfactory results are obtained.
 - 4. Submit written copies of test results.

END

OFFICE OF PUBLIC SAFETY/POLICE
Technology Services Division
Integrated Security Management Specifications

University of the District of Columbia
4200 Connecticut Ave., NW | Washington, DC 20008
Administration Building (39), Suite C04
D: 202.274.5282 | F: 202.274.7486
www.udc.edu/police