METROPOLITAN EXPOSITION RECREATION COMMISSION

RESOLUTION NO. 14-28

For the purpose of selecting Convergint Technologies, LLC., for the Oregon Convention Center – "Integrated Electronic Security Upgrade" and authorizing the Deputy Chief Operating Officer of Metro to execute a contract with Convergint Technologies, LLC.

WHEREAS, the Oregon Convention Center's (OCC) Security Camera and Access Control systems have reached the end of their useful life and require replacement; and

WHEREAS, MERC staff has worked with a security consultant to design a new integrated system to allow both systems to be operated more efficiently by security staff; and

WHEREAS, the project is included in the fiscal year 15 capital plan; and

WHEREAS, Section 4(D) of the Metropolitan Exposition Recreation Commission's ("MERC") Contracting and Purchasing Rules allows procurement of goods or services of $100,000 or more to be awarded through issuance of competitive sealed proposals, in accordance with the provisions of ORS 279B.060; and

WHEREAS, MERC staff has evaluated the proposals and has selected Convergint Technologies as the most responsive and responsible proposer with a proposal amount of three hundred, thirty-seven thousand, nine hundred ninety-seven and no/100th dollars ($337,997.00)

BE IT THEREFORE RESOLVED as follows:

1. MERC selects Convergint Technologies, LLC., as the most responsive and responsible proposer in response to the Request for Proposals for the Oregon Convention Center – Integrated Electronic Security Upgrade.

2. MERC approves the contract with Convergint Technologies, LLC., in the form substantially similar to the attached Exhibit A and authorizes the Deputy Chief Operating Officer of Metro to execute the contract on behalf of the Commission.

Passed by the Commission on November 5, 2014.

Chair

Secretary/Treasurer

Approved As to Form:
Alison R. Kean, Metro Attorney

By: _____
Nathan A. S. Sykes
Deputy Metro Attorney

MERC STAFF REPORT

Agenda Item/Issue: For the purpose of selecting Convergint Technologies, LLC., for the Oregon Convention Center (OCC) -"Integrated Electronic Security Upgrade" and authorizing the Deputy Chief Operating Officer of Metro to execute a contract with Convergint Technologies, LLC.

Resolution No: 14-28 **Presented by:** Scott Cruickshank

Date: November 5, 2014

Background and Analysis: The OCC's current security camera and access control systems are over ten years old, unsupported and in need of replacement.

The OCC has an overall Physical Security Information Management Plan to upgrade security. This plan requires an upgrade of the existing security video management system, replacement of the existing Access Control System, integrating the new video system with the new Access Control System, and upgrade of the security console in the Security Operations Center.

The OCC utilizes 24/7 security staff to handle numerous tasks in both the Security Operations Center and on the main facility floor. From the Center by the west freight dock, staff control facility lighting systems; monitor security video cameras, intercoms and fire detection systems; and manage access to roll-up doors, card readers and controlled public entrances. Outside of the security center, security staff patrol, respond to alarms, and assist exhibitors and the public.

The OCC wants to digitize and migrate their current analog cameras to a new video monitoring system. This new system was selected by Metro as the standard for the organization and would allow the OCC to add high resolution video cameras during the upgrade.

The OCC's current Access Control System has reached its end-of-life. The funds for a replacement were budgeted in the FY 16 capital plan, however including this replacement with the video management project is a more efficient installation. OCC needs to replace its old Access Control System to allow integration with the new video monitoring system to use an established application programming interface software between the two systems. This will give the OCC the ability to view and monitor system alarms and related video segments from one workstation computer monitor.

With the transition to fully integrated video monitoring and access control systems, the OCC's security center will need an upgrade. This would include a new security console, four large digital video wall-monitors to manage the increased number of security cameras, and an improved arrangement of its various monitoring systems to address ergonomic concerns. The work performed under this contract will provide the OCC with the initial infrastructure necessary for future expansion of these systems as required by venue needs.

MERC Staff prepared and issued proposal documents and a Request for Proposals in accordance with MERC's purchasing policies for the Oregon Convention Center (OCC) -"Integrated Electronic Security Upgrade." In the proposal documents, MERC staff included requirements of a good faith effort for outreach to the MWESB and FOTA communities. In addition to these requirements, the RFP was published in the Asian Reporter, the DJC, and ORPIN.

On July 24, 2014, MERC Staff conducted a site walk for potential bidders in which ten security contractors and two subcontractors attended: Two subcontractors were ESBs, none were WBE, MBE or FOTA. Three proposals were received on August 19, 2014. One proposal was received from an ESB firm. The winning proposer was Convergint Technologies, LLC, for a contract amount of three hundred, thirty-seven thousand, nine hundred ninety-seven & 00/100 dollars ($337,997.00). The winning proposer Convergint Technologies, LLC, is neither an MWESB firm nor is it located in the FOTA but it did include two MWESB subcontractors for this project.

FISCAL IMPACT: This project has a budget of $230,000.00 in FY 2015. There is enough budget appropriation authority in the MERC Fund to approve the entire contract amount in FY 2015. The budget shortfall will be funded though a contribution from the Aramark Reserve account and savings from Phase II of the Roof Replacement Project. OCC staff planned for a contribution of $55,000.00 from the Aramark Reserve fund to provide for cameras requested by Aramark.

RECOMMENDATION: Staff recommends that the Metropolitan Exposition-Recreation Commission, by Resolution No. 14-28, approve the contract award and written contract (attached hereto) with Convergint Technologies, LLC., for the amount of three hundred, thirty-seven thousand, nine hundred ninety-seven & 00/100 dollars ($337,997.00) for the Oregon Convention Center (OCC) -"Integrated Electronic Security Upgrade."

Metro | Exposition Recreation Commission
600 NE Grand Ave., Portland, OR 97232-2736
503-797-1700

Standard Public Contract

MERC CONTRACT NO. 305006

For Public Contracts $50,000 & Above

THIS Contract is entered into between Metropolitan Exposition Recreation Commission (MERC), an appointed commission of Metro, whose address is 600 NE Grand Avenue, Portland, Oregon 97232-2736, and Convergint Technologies, LLC, whose address is 16575 SW 72nd Ave, Portland, OR 97224, hereinafter referred to as the "CONTRACTOR."

THE PARTIES AGREE AS FOLLOWS:

ARTICLE I
SCOPE OF WORK

CONTRACTOR shall perform the work and/or deliver to MERC the goods described in the Scope of Work attached hereto as Attachment A. All services and goods shall be of good quality and, otherwise, in accordance with the Scope of Work.

ARTICLE II
TERM OF CONTRACT

The term of this Contract shall be for the period commencing November 12, 2014, through and including May 29, 2015, with substantial completion by April 30, 2015. This agreement may be amended or extended at MERC's sole discretion.

ARTICLE III
CONTRACT SUM AND TERMS OF PAYMENT

MERC shall pay the CONTRACTOR for work performed and/or goods supplied as described in the Scope of Work, in the maximum amount of THREE HUNDRED THIRTY-SEVEN THOUSAND, NINE HUNDRED NINETY-SEVEN AND NO/100TH DOLLARS ($337,997.00)(the "Maximum Price").

Itemized Pricing and Hourly Rates per Pricing Schedule hereto attached as Attachment F

MERC shall not be responsible for payment of any materials, expenses or costs other than those which are specifically included in the Scope of Work. The Maximum Price includes all fees, costs and expenses of whatever nature. Each of MERC's payments to Contractor shall equal the percentage of the work Contractor accomplished during the billing period. Contractor's billing invoices shall include the MERC contract number, Contractor name, remittance address, invoice date, invoice number, invoice amount, tax amount (if applicable), and an itemized statement of work performed and expenses incurred during the billing period, and will not be submitted more frequently than once a month.

Contractor's billing invoices shall be sent to Metro Accounts Payable, 600 NE Grand Avenue, Portland, OR 97232-2736 or metroaccountspayable@oregonmetro.gov. The MERC contract number shall be referenced in the email subject line. Contractor's billing invoices for services through June 30 shall be submitted to Metro by July 15. Payment shall be made by MERC on a Net 30 day basis upon approval of CONTRACTOR invoice.

ARTICLE IV
LIABILITY AND INDEMNITY

CONTRACTOR is an independent contractor and assumes full responsibility for the content of its work and performance of CONTRACTOR'S labor, and assumes full responsibility for all liability for bodily injury or physical damage to person or property arising out of or related to this Contract, and shall indemnify, defend and hold harmless MERC, its agents and employees, from any and all claims, demands, damages, actions, losses, and expenses arising out of or in any way connected with its performance of this Contract. CONTRACTOR is solely responsible for paying CONTRACTOR'S subcontractors and nothing contained herein shall create or be construed to create any contractual relationship between any subcontractor(s) and MERC. Such indemnification by Licensee shall apply unless such damage or injury results from the lose negligence or willful misconduct of MERC or Metro. In no event shall either Convergint or customer be liable to the other party hereto for special, indirect, incidental, or consequential damages, including commercial loss, loss of use or lost profits, even if that party has been advised of the possibility of such damages

In no event shall either Convergint or customer be liable to the other party hereto for indirect, incidental, or consequential damages, including commercial loss, loss of use or lost profits, even if that party has been advised of the possibility of such damages.

ARTICLE V
TERMINATION

MERC may terminate this Contract upon giving CONTRACTOR seven (7) days written notice. In the event of termination, CONTRACTOR shall be entitled to payment for work performed to the date of termination. MERC shall not be liable for indirect, consequential damages or any other damages. Termination by MERC will not waive any claim or remedies it may have against CONTRACTOR.

ARTICLE VI
INSURANCE & BONDS

CONTRACTOR shall purchase and maintain at the CONTRACTOR'S expense, the following types of insurance, covering the CONTRACTOR, its employees, and agents:

A. The most recently approved ISO (Insurance Services Office) Commercial General Liability policy, or its equivalent, written on an occurrence basis, with limits not less than $1,000,000 per occurrence and $1,000,000 aggregate. The policy will include coverage for bodily injury, property damage, personal injury, contractual liability, premises and products/completed operations. CONTRACTOR'S coverage will be primary as respects METRO;
B. Automobile insurance with coverage for bodily injury and property damage and with limits not less than minimum of $1,000,000 per occurrence;
C. Workers' Compensation insurance meeting Oregon statutory requirements including Employer's Liability with limits not less than $500,000 per accident or disease; and
D. Professional Liability Insurance, with limits of not less than $1,000,000 per occurrence, covering personal injury and property damage arising from errors, omissions or malpractice.

METRO, MERC, its elected officials, departments, employees, and agents shall be named as ADDITIONAL INSUREDS on Commercial General Liability and Automobile policies.

CONTRACTOR shall provide to MERC 30 days notice of any policy cancellation.

CONTRACTOR shall provide MERC with a Certificate of Insurance complying with this article upon return of the CONTRACTOR signed agreement to MERC. Certificate of Insurance shall identify the MERC contract number.

CONTRACTOR shall not be required to provide the liability insurance described in this Article only if an express exclusion relieving CONTRACTOR of this requirement is contained in the Scope of Work.

In addition, for public works subject to ORS 279C.800 to 279C.870, CONTRACTOR and every subcontractor shall have a public works bond required by 2005 Oregon Laws Chapter 360 filed with the Construction Contractors Board before starting work on the project, unless exempt under Section 2 of 2005 Oregon Laws Chapter 360.

ARTICLE VII
PUBLIC CONTRACTS

All applicable provisions of ORS chapters 187 and 279A, 279B, and 279C and all other terms and conditions necessary to be inserted into public contracts in the State of Oregon, are hereby incorporated as if such provision were a part of this Agreement. Specifically, it is a condition of this contract that CONTRACTOR and all employers working under this Agreement are subject employers that will comply with ORS 656.017 as required by 1989 Oregon Laws, Chapter 684.

For public work subject to ORS 279C.800 to 279C.870, the CONTRACTOR shall pay prevailing wages. If such public work is subject both to ORS 279C.800 to 279C.870 and to 40 U.S.C. 276a, the CONTRACTOR and every subcontractor on such public work shall pay at least the higher prevailing wage. The CONTRACTOR and each subcontractor shall pay workers not less than the specified minimum hourly rate of wage in accordance with Section 7 of

2005 Oregon Laws Chapter 360. MERC shall pay an administrative fee as provided in ORS 279C.825(1) to the Bureau of Labor and Industries pursuant to the administrative rules established by the Commissioner of Labor and Industries. CONTRACTORS must promptly pay, as due, all persons supplying to such contractor labor or material used in this contract. If the CONTRACTOR or first-tier subcontractor fails, neglects, or refuses to make payment to a person furnishing labor or materials in connection with the public contract for a public improvement within 30 days after receipt of payment from the public contracting agency or a contractor, the CONTRACTOR or first-tier subcontractor shall owe the person the amount due plus shall pay interest in accordance with ORS 279C.515. If the CONTRACTOR or first-tier subcontractor fails, neglects, or refuses to make payment, to a person furnishing labor or materials in connection with the public contract, the person may file a complaint with the Construction Contractors Board, unless payment is subject to a good faith dispute as defined in ORS 279C.580. CONTRACTOR must pay any and all contributions and amounts due to the Industrial Accident Fund from contractor or subcontractor and incurred in the performance of the contract. No liens or claims are permitted to be filed against MERC on account of any labor or material furnished. CONTRACTORS are required to pay the Department of Revenue all sums withheld from employees pursuant to ORS 316.167.

For public improvement work all CONTRACTORS must demonstrate that an employee drug-testing program is in place.

ARTICLE VIII
MODIFICATIONS

MERC may approve changes and modifications to the original contract, including deletions of work, order of additional materials, and additional services reasonably related to the original work scope. Contractor may propose changes in the work that Contractor believes are necessary, will result in higher quality work, improve safety, decrease the amount of the contract, or otherwise result in a better or more efficient work product. If such changes are approved by MERC, they shall be executed by written contract amendment signed by both parties. Such changes shall not relieve Contractor of any obligation or warranty under the contract. No oral statements by either party shall modify or affect the terms of the contract.

ARTICLE IX
QUALITY OF GOODS AND SERVICES

Unless otherwise specified, all materials shall be new and both workmanship and materials shall be of the highest quality. All workers and subcontractors shall be skilled in their trades. CONTRACTOR guarantees all work against defects in material or workmanship for a period of one (1) year from the date of acceptance or final payment by MERC, whichever is later. All guarantees and warranties of goods furnished to CONTRACTOR or subcontractors by any manufacturer or supplier shall be deemed to run to the benefit of MERC.

ARTICLE X
OWNERSHIP OF DOCUMENTS

Unless otherwise provided herein, all documents, instruments and media of any nature produced by CONTRACTOR pursuant to this agreement are Work Products and are the property of MERC, including but not limited to: drawings, specifications, reports, scientific or theoretical modeling, electronic media, computer software created or altered specifically for the purpose of completing the Scope of Work, works of art and photographs. Unless otherwise provided herein, upon MERC request, CONTRACTOR shall promptly provide MERC with an electronic version of all Work Products that have been produced or recorded in electronic media. MERC and CONTRACTOR agree that all work Products are works made for hire and Contractor hereby conveys, transfers, and grants to MERC all rights of reproduction and the copyright to all such Work Products.

A. CONTRACTOR and subcontractors shall maintain all fiscal records relating to such contracts in accordance with generally accepted accounting principles. In addition, CONTRACTOR and subcontractors shall maintain any other records necessary to clearly document:

1. The performance of the CONTRACTOR, including but not limited to the contractor's compliance with contract plans and specifications, compliance with fair contracting and employment programs, compliance with Oregon law on the payment of wages and accelerated payment provisions; and compliance with any and all requirements imposed on the CONTRACTOR or subcontractor under the terms of the contract or subcontract;

2. Any claims arising from or relating to the performance of the CONTRACTOR or subcontractor under a public contract;
3. Any cost and pricing data relating to the contract; and
4. Payments made to all suppliers and subcontractors.

B. CONTRACTOR and subcontractors shall maintain records for the longer period of (a.) six years from the date of final completion of the contract to which the records relate or (b.) until the conclusion of any audit, controversy or litigation arising out of or related to the contract.

C. CONTRACTOR and subcontractors shall make records available to METRO, and its authorized representatives, including but not limited to the staff of any METRO department and the staff of the METRO Auditor, within the boundaries of the METRO region, at reasonable times and places regardless of whether litigation has been filed on any claims. If the records are not made available within the boundaries of METRO, the CONTRACTOR or subcontractor agrees to bear all of the costs for METRO employees, and any necessary consultants hired by METRO, including but not limited to the costs of travel, per diem sums, salary, and any other expenses that Metro incurs, in sending its employees or consultants to examine, audit, inspect, and copy those records. If the CONTRACTOR elects to have such records outside these boundaries, the costs paid by the CONTRACTOR to METRO for inspection, auditing, examining and copying those records shall not be recoverable costs in any legal proceeding.

D. CONTRACTOR and subcontractors authorize and permit METRO and its authorized representatives, including but not limited to the staff of any METRO department and the staff of the METRO Auditor, to inspect, examine, copy and audit the books and records of CONTRACTOR or subcontractor, including tax returns, financial statements, other financial documents and any documents that may be placed in escrow according to any contract requirements. METRO shall keep any such documents confidential to the extent permitted by Oregon law, subject to the provisions of section E.

E. CONTRACTOR and subcontractors agree to disclose the records requested by METRO and agree to the admission of such records as evidence in any proceeding between METRO and the CONTRACTOR or subcontractor, including, but not limited to, a court proceeding, arbitration, mediation or other alternative dispute resolution process.

F. CONTRACTOR and subcontractors agree that in the event such records disclose that METRO is owed any sum of money or establish that any portion of any claim made against Metro is not warranted, the CONTRACTOR or subcontractor shall pay all costs incurred by METRO in conducting the audit and inspection. Such costs may be withheld from any sum that is due or that becomes due from METRO.

G. Failure of the CONTRACTOR or subcontractor to keep or disclose records as required by this document or any solicitation document may result in disqualification as a bidder or proposer for future METRO contracts as provided in ORS 279B.130 and Metro Code Section 2.04.070(c), or may result in a finding that the CONTRACTOR or subcontractor is not a responsible bidder or proposer as provided in ORS 279B.110 and Metro Code Section 2.04.052.

ARTICLE XI
SUBCONTRACTORS

CONTRACTOR shall contact MERC prior to negotiating any subcontracts and CONTRACTOR shall obtain approval from MERC before entering into any subcontracts for the performance of any of the services and/or supply of any of the goods covered by this Contract.

MERC reserves the right to reasonably reject any subcontractor or supplier and no increase in the CONTRACTOR'S compensation shall result thereby. All subcontracts related to this Contract shall include the terms and conditions of this agreement. CONTRACTOR shall be fully responsible for all of its subcontractors as provided in Article IV.

ARTICLE XII
RIGHT TO WITHHOLD PAYMENTS

MERC shall have the right to withhold from payments due CONTRACTOR such sums as necessary, in MERC's sole opinion, to protect MERC against any loss, damage or claim which may result from CONTRACTOR'S performance or failure to perform under this agreement or the failure of CONTRACTOR to make proper payment to any suppliers or subcontractors. In addition for public improvement work, if a CONTRACTOR is required to file certified statements under ORS 279C.845, MERC shall retain 25 percent of any amount earned by the CONTRACTOR on the public works until the contractor has filed all required certified statements with MERC.

If a liquidated damages provision is contained in the Scope of Work and if CONTRACTOR has, in MERC's opinion, violated that provision, MERC shall have the right to withhold from payments due CONTRACTOR such sums as shall satisfy that provision. All sums withheld by MERC under this Article shall become the property of MERC and CONTRACTOR shall have no right to such sums to the extent that CONTRACTOR has breached this Contract.

ARTICLE XIII
SAFETY

If services of any nature are to be performed pursuant to this agreement, CONTRACTOR shall take all necessary precautions for the safety of employees and others in the vicinity of the services being performed and shall comply with all applicable provisions of federal, state and local safety laws and building codes, including the acquisition of any required permits.

ARTICLE XIV
INTEGRATION OF CONTRACT DOCUMENTS

All of the provisions of any procurement documents including, but not limited to, the Advertisement for Bids, Proposals or responses, General and Special Instructions to Bidders, Proposal, Scope of Work, and Specifications which were utilized in conjunction with the bidding of this Contract are hereby expressly incorporated by reference. Otherwise, this Contract represents the entire and integrated agreement between MERC and CONTRACTOR and supersedes all prior negotiations, representations or agreements, either written or oral. This Contract may be amended only by written instrument signed by both MERC and CONTRACTOR. The laws of the state of Oregon shall govern the construction and interpretation of this Contract.

ARTICLE XV
COMPLIANCE

CONTRACTOR shall comply with federal, state, and local laws, statutes, and ordinances relative to the execution of the work. This requirement includes, but is not limited to, non-discrimination, safety and health, environmental protection, waste reduction and recycling, fire protection, permits, fees and similar subjects.

ARTICLE XVI
INTERGOVERNMENTAL COOPERATIVE AGREEMENT

Pursuant to ORS 279A and the Metro public contract code, Metro participates in an Intergovernmental Cooperative Purchasing program by which other public agencies shall have the ability to purchase the goods and services under the terms and conditions of this awarded contract. Any such purchases shall be between the Contractor and the participating public agency and shall not impact the Contractor's obligation to Metro under this agreement. Any estimated purchase volumes listed herein do not include volumes for other public agencies, and Metro makes no guarantee as to their participation in any purchase. Any Contractor may decline to extend the prices and terms of this solicitation to any or all other public agencies upon execution of this contract. Unless the Contractor specifically declines to participate in the program by marking the box below, the Contractor agrees to participate in the Intergovernmental Cooperative Purchasing program. **Contractor declines to participate in the Intergovernmental Cooperative Purchasing program or is not applicable to this Contract as indicated by the following initials _____.**

ARTICLE XVII
SITUS

The situs of this Agreement is Portland, Oregon. Any litigation over this agreement shall be governed by the laws of the State of Oregon and shall be conducted in the Circuit Court of the state of Oregon for Multnomah County, or, if jurisdiction is proper, in the U.S. District Court for the District of Oregon.

ARTICLE XVIII
ASSIGNMENT

CONTRACTOR shall not assign any rights or obligations under or arising from this Contract without prior written consent from MERC.

ARTICLE XIV
SEVERABILITY

The parties agree that any provision of this Contract that is held to be illegal, invalid, or unenforceable under present or future laws shall be fully severable. The parties further agree that this Contract shall be construed and enforced as if the illegal, invalid, or unenforceable provision had never been a part of them and the remaining provisions of the Contract shall remain in full force and effect and shall not be affected by the illegal, invalid, or unenforceable provision or by its severance from this Contract. Furthermore, a provision as similar to the illegal, invalid, or unenforceable provision as is possible and legal, valid and enforceable shall be automatically added to this Contract in lieu of the illegal, invalid, or unenforceable provision. Any failure by MERC to enforce a provision of the Contract is not to be construed as a waiver by MERC of this right to do so.

ARTICLE XX
COUNTERPARTS

This Contract may be executed in counterparts or multiples, any one of which will have the full force of an original.

ARTICLE XXI
DELIVERY OF NOTICES

Any notice, request, demand, instruction, or any other communications to be given to any party hereunder shall be in writing, sent by registered or certified mail or fax as follows:

To Contractor: Anthony Wilson
Convergint Technologies, LLC
16575 SW 72nd Ave
Portland, OR 97224
503-228-8521 fax

To Metro: Metro Procurement Services
600 NE Grand Ave
Portland, Oregon 97232
503-797-1791 fax

With Copy to: Josh Lipscomb
600 NE Grand Ave
Portland, OR 97232
503-797-1795 fax

CONTRACTOR

By_____

Print Name_____

Date_____

METROPOLITAN EXPOSITION RECREATION COMMISSION

By_____

Print Name_____

Date_____

MERC Contract No. 305006

1. Purpose and Goal of Work

MERC is contracting for an Integrated Electronic Security Upgrade for The Oregon Convention Center (OCC), located at 777 NE MLK Jr. Blvd, Portland, OR 97232. Contractor shall complete an upgrade of the OCC's existing Video Management System (VMS), replace the existing Access Control System (ACS), integrate the upgraded VMS with the new ACS, and upgrade the Security Operations Center (SOC). Contractor is to furnish and install all materials listed in the contract and provide all labor necessary for execution of all work as described in the scope of work, unless otherwise stated.

2. Description of the Scope of Work

In this Contract's Scope of Work, Metro's On-Net Surveillance Systems Inc. (OnSSI) VMS licenses will be upgraded/added in the following 6 step process:

1. Metro's PS Base License and PS Camera Licenses will be abandoned.
2. Metro's IS Base License will be upgraded from 32bit "IS" to 64bit "LS".
3. Two (2) OCC "LS" recording server licenses will be provided for 2 new recording servers supplied by Metro. (*Of Metro's (80) existing 32bit IS camera channel licenses, all 80 IS camera licenses will remain on Metro's Zoo "IS" recording server and will not be upgraded to LS.)*
4. Ninety six (96) new 64bit "LS" camera channel licenses will be added to the OCC recording servers (operating under Metro's upgraded LS Base License) to support OCC's baseline requirements of this contract.
5. An additional 14 "LS" camera channel license will be added for each OCC "Optional" camera selected.
6. All new or upgraded OnSSI "LS" licenses will have an OnSSI "Current" software upgrade plan that is prorated to coincide with Metro's existing Feb 7, 2015 "Current" renewal date.

Of its 73 existing analog cameras, OCC's security camera requirement includes removing one (1) camera (from the north shipping dock area), replacing eight (8) others with new MegaPixel (MP) digital cameras, and converting the remaining 64 analog cameras to digital with H.264 Encoders. For ease of installation, new H.264 encoders will be installed in the current rack provided for the Kalatel equipment. The Kalatel equipment will be removed once all cameras are migrated to the OnSSI VMS. Of the analog cameras that are converted to digital, twelve (12) will require some servicing or adjustment. This conversion project will add seventy-three (73) existing cameras (64 analog and 9 digital) to OCC's new "LS" recording servers. Additionally OCC will add thirty-seven (37) new digital cameras. The total security cameras being recorded on OCC's new OnSSI LS recording servers under this system upgrade will be one hundred ten (110) cameras. All new LS camera channel licenses for OCC will be provided with software upgrade "Current" plans prorated to Metro's Feb 7, 2015 renewal date, including any accepted alternate cameras.

A.1 Security Access Control System (ACS) Replacement

OCC currently operates an Infographics Diamond II ACS that has reached its product "end-of-life". OCC needs the system replaced with a leading ACS that is capable of offering the feature set and future expansion of the card reader system at OCC. iClass SE Card Readers and Credentials will be utilized. The S2 ACS selected will be integrated with the OnSSI Video Management System with a proven, off-the-shelf API for integrating video segments and video control from within the ACS alarm report screen.

OCC's existing Diamond II system utilizes ACUs (Access Control Units) as "Network Intelligent Controllers" that communicate with RREs (Remote Reader Electronics) at the door for card reader control, RIMs (Remote Input Modules), and RRMs (Remote Relay Modules). There are a total 4 ACU's, 14 RIMs, 16 RREs, and 2 RRMs. Two of the RREs are installed next to the ACU-0 at the P2 Parking office, and the rest of the RIMs, RREs, and RRMs are installed near the doors they control or monitor. The system also monitors 14 sets of glass entry and rollup doors with each set comprised of 4

to 6 doors. Refer to the "OCC's Existing Diamond II ACS Configuration" document included as Attachment D for detailed information. Where feasible contractor will reuse the existing ACS cabling and enclosures. The Diamond II system currently controls 16 card readers and 33 individual rollup doors and parking gates remotely from a graphic map. These card readers will be replaced with HID iClass RP40 Wall Switch Readers.

Alternate #18 from the RFP has been accepted by MERC will provide equipment and installation of the Mercury card reader controllers, power supplies, input/output boards, and other system elements required to replicate the functions of the existing Diamond II ACS.

ACS Installation Approach

OCC will remove the Diamond II controller boards from each of the ACU, RIM, RRE, and RIM enclosures and label each connecting cable. Contractors will assume that all existing cabling and enclosures can be reutilized. Contractor will be responsible for removing power supplies and replacing with new. As most of the RIMS, RREs, and RRMs are mounted high above the doors they monitor, Contractor will provide a high-lift for removal and replacement of the ACS controllers.

The Contractor shall schedule the removal of the Diamond II controllers by OCC's designated technician with the installation of the new ACS controllers by the Contractor. Contractor shall schedule work to minimize delays during this changeover.

A.2 Integration of the upgraded Video System with the replaced Access Control System

The integration of the OnSSI VMS with the new ACS will be accomplished through the use of established "off-the-shelf" Application Programming Interface (API) software that will provide data sharing between the two systems. Each of these systems is a separate distinct system, they will communicate with each other with an API "data bridge" that allows them to share alarm and video information. This API will allow OCC to automatically monitor related security video clips from the ACS alarm record without having to search both systems independently.

A.3 Security Operations Center (SOC) Upgrade

Contractor is to provide and install a new security console and camera viewing station. The new design incorporates a Winsted security console with additional cabinetry, and four (4) "46" LCD wall computer monitors for viewing selected security camera video. These monitors are arranged in a "V" configuration in the NW corner of the SOC.

The Kalatel DVRs and a Digiplex Matrix Switcher are rack mounted in an equipment room in the SOC. Contractor will remove and replace the Kalatel equipment with rack mounted H.264 Encoders which will be mounted in the existing rack. A digital joystick will be provided for the new OnSSI VMS view station to be located in the NW corner of the SOC. The joystick will also have a camera selection feature for displaying security camera video on any one of the four new 46" HD LCD monitors to be mounted in the NW corner of the SOC.

Photos of the existing SOC with drawings of the redesigned SOC are provided in Attachment D

A.4 General Instructions

1. OCC's OnSSI VMS shall be upgraded from an "IS" Base license to a "LS" Base License, and integrated with the new ACS using an established and proven API so that alarm related security video segments can be linked to the ACS alarm record and viewed from a single computer monitor.

2. Contractor will reuse all serviceable electronic door locking hardware, motion detectors, and door position switches. Existing ACS and VMS cable will be reutilized where feasible. Where existing Coax cable can be used for new IP network cameras, video-over-coax converters will be used.
3. Contractor will replace the existing card readers with new HID iClass SE card readers.
4. Contractor will assume that existing ACS cabling to the reader, door locks, and door sensors is in good condition to support the new ACS.
5. Any additional cabling required to support the new ACS will be provided and installed by the Contractor.
6. Contractor is responsible for properly recycling or disposing of the outdated ACS or VMS related equipment it removes and replaces.
7. The new ACS controllers will be Mercury controllers to ensure availability from multiple commercial suppliers across various ACS platforms.
8. All new camera cable must be Cat 6, color coded and approved by Metro's Information Systems Department. OCC has standardized on CAT 6 cable for its camera and LAN requirements.
9. New ACS card readers will be HID iCLASS SE with the model appropriate for the location (i.e. mullion readers for glass storefronts and wall switch readers for hallways, entrances, and gates).
10. Contractor will provide one (1) ACS video ID badge station client software, ID badge camera, and ID Badge Printer. The Badge client will be installed on an existing OCC work station. The ID Badge Printer will be a dual sided ID ISO-30 badge printer. The ID Badge printer shall be a Magicard Rio Pro or Fargo DTC1250e.
11. OCC will require 1000 of the iCLASS SE photo printable contactless Smart Card ID badge card stock for its ACS ID Badge Client.
12. Contractor will provide eleven (11) ACS and VMS administrative clients for OCC's existing desktop workstations for system administrators
13. Where existing ACS doors are monitored for door position, that monitoring will continue with the new ACS.
14. LAN UPS equipment, if needed, will be provided by OCC.
15. Contractor will provide new power supplies and a minimum of one hour of battery backup for all ACS panels.
16. Existing security cameras will continue to utilize existing power supplies.
17. Existing composite cameras scheduled for conversion to digital format will utilize an H.264 video encoder for conversion to digital for migration to the OnSSI VMS.
18. OCC will provide standard LAN switches, and PoE LAN switches for camera LAN connectivity to the LAN and to provide power to new cameras that are PoE,
19. Circuit protection will be provided for all ACS panels. Lightning and surge protection will be provided for all VMS and ACS equipment susceptible to such conditions.
20. Contractor will provide 1-year software support agreement for the ACS. Contractor will also provide software support for new components of the upgraded OnSSI VMS system to include the upgraded base management software and new component licensing (i.e. camera licenses) prorated to Feb 7, 2015.

21. In addition to routine service for the equipment it installs, Contractor will provide 4 hr "Emergency Response" for critical service support as requested by OCC, or next day "Priority Service" as requested by OCC.

22. Four (4) VMS Smart Phone Apps will be provided for OCC Staff to monitor video remotely from their smart phones.

23. The Warranty period for new ACS and VMS system and its components will be as provided by the Manufacturer.

A.5 Material Requirements

Contractor will:

1. Provide and install all materials and products per manufacturer's specifications.

2. Where test standards exist, all electronic products furnished by the contractor for construction shall be UL listed by a national recognized testing agency to meet the requirements of State of Oregon Electrical Code. All material, products, and components furnished by the contractor shall be manufactured, assembled, installed, and tested in accordance with the current industry standards.

3. All equipment, labor and materials shall be provided by the contractor except as noted below or elsewhere in this document.
   a. Equipment/Items provided by OCC:
      i. Telecommunication ground bus bar (TGB)
      ii. Desktop Workstations (PCs with MS/OS clients)
      iii. (2) OCC VMS Recording Servers.
      iv. UPS power supplies for Recording Servers and LAN switches.
      v. Server Racks
      vi. Grounding materials and labor for the server cabinets
      vii. Facility Floor Plans in electronic format for use with VMS camera location graphics
      viii. Paint and Patching required as a result of card reader replacement
   b. Contractor requirements:
      i. Power supplies and backup batteries for the new ACS will be new equipment, and provided by the Contractor.

OCC will:

1. Remove all existing wall cabinets and relocate the fire panel and other facility control panels in the SOC as required for the new security console.

A.6 Documentation Contractor to Provide

Contractor shall provide documentation to OCC as specified in this section:

1. Product Samples/Cut sheets - Contractor shall submit to MERC's Project Manager or designee for approval all specification sheets of equipment/cameras/encoders/video monitor and computer to be installed.

2. Project Plan - Contractor shall brief MERC's Project Manager or designee on a project plan, which will include all tasks required to successfully complete the project, with responsibility, due date, and expected time frames required to complete each task (by site), based on the current schedule. This plan shall coordinate the contractor's required tasks with OCC's scheduling requirements.

3. Project As-built Drawings – OCC will provide CAD baseline drawings. Contractor is required to provide final "As-built" electronic CAD drawings to MERC's Project Manager which document all

the components installed connected with this proposal. Contractor shall provide electronic copies denoting final device/equipment placement.

A.7 Minimum Requirements

1. Project Management - Contractor shall provide a project manager throughout the course of the installation to provide coordination of work, to work with MERC, and provide technical information when requested. This person(s) shall be responsible for quality control during installation and testing.
2. Project Meetings - The Contractor's on-site project manager shall attend the kick-off meeting and weekly update meetings, and other required project meetings throughout the project to ensure good coordination with work related activities.
3. Inspections – Contractor's Project Manager shall attend all site inspections as requested by the OCC Project Manager.
4. Work Standards - All work shall be accomplished in strict conformity with all applicable building codes, laws and ordinances.
5. Permits, License, and Inspection Fees - Contractor must be licensed to perform work at OCC, and shall prepare and submit to all authorities having jurisdiction, all applications and working drawings as required. Contractor shall obtain all necessary permits and certificates of compliance or approval and deliver these to OCC; OCC is enrolled in the facility permit program with the city of Portland and as such will pay for all permits.
6. Service Disruption - Contractor will make every diligent effort to avoid disruption of services or business activities at OCC. Contractor will advise the MERC Project Manager or designee in a timely manner if service must be disrupted to accomplish the scope of work. Contractor will coordinate cut-over's with already scheduled down times and be well prepared to meet downtime schedule.
7. New Equipment - All equipment furnished by the contractor shall be new, unused and currently in regular production.
8. All electrical equipment components and cameras shall be UL listed by a national recognized testing agency to meet the requirements of State of Oregon Electrical Code.
9. Any items omitted from this contract that are clearly necessary for the operation of such equipment, although not directly specified or called for in these specifications, shall be considered a portion of such equipment.
10. Unacceptable Activities
    a. No alcoholic beverages, illegal drugs, illegal activities, etc. will be permitted on OCC premises.
    b. When requested by OCC, Contractor shall remove from the premises any of its employees or subcontractors who are abusive, harassing, or insubordinate to OCC, their employees, agents, consultants, Contractors, or are suspect for the use of drugs and/or alcohol.
11. Debris Removal
    a. Contractor shall maintain a clean work site of debris such as pallets, cable scraps, packaging, etc. These items shall be removed daily.
    b. To support the OCC's sustainability goals, materials being removed from the worksite shall be recycled and receipts provided to the OCC project manager. If recycling is not possible, then approval must be obtained from the OCC's project manager for disposal.

A.8 Recommended Project Installation Approach

In an effort to reduce delays in OCC's security system function and monitoring, the following installation steps are recommended for this project:

1. Contractor will initially start with the upgrade of the OCC SOC. This step will include installing a new security console and four 46" LED wall monitors. The 10 existing analog monitors mounted in the SE corner of the SOC are housed in a cabinet that is currently mounted to the existing security desk. Contractor will arrange for a temporary support for that cabinet while the existing security desk is removed and replaced with the new security console. The 10 analog monitors will continue to function normally until all OCC analog cameras are converted to digital. The four 46" HD LED wall monitors will be provided and mounted by the Contractor on floor mounts purchased from Winsted as part of the new security console.
2. In preparation for the SOC upgrade, OCC will remove the wall mounted cabinets at the NW corner and the floor cabinet on the east wall. OCC will raise the existing fire panel on the west wall by 11" so as to keep it visible above a desk monitor scheduled for that area. OCC will relocate facility system control panels on the west wall of the SOC as necessary. All other desktop equipment and computers will remain in-place until such time as OCC schedules the relocation of that desktop equipment. OCC to provide all computers and computer monitors.
3. After the new security console has been installed and the four new video wall in the NW corner are functional, control for the single existing digital camera on the OnSSI VMS will be migrated to those new monitors.
4. Contractor will then commence the process of converting the existing analog cameras to digital. As that process continues, the rack mounted Kalatel DVRs and Matrix Switcher in the SOC will be replaced with rack mounted H.264 Video Encoders in the SOC equipment room. This approach should allow a minimum of cable rework during the conversion process.
5. Rough-in cabling for new cameras will commence at the discretion of the Contract on approval from the OCC Project Manager.
6. Unless an earlier date is approved by the OCC Project Manager, conversion of the Diamond II ACS will be the delayed until after the camera system upgrade has been completed. During the ACS conversion, it is recommended that the new ACS network communication controllers be assigned a different LAN IP address than the existing ACUs so as to allow the Diamond II ACS to continue to operate normally as its ACU panels are replaced. Since there are four Diamond II ACUs involved with each located in a different quadrant of OCC, it is recommended that the conversion of the ACS proceed in a 4-step process of converting one ACU panel and its related subpanels at a time before moving to the next ACU. This 4-step process must be carefully coordinated with the OCC designated technician that is tasked with ACU removal. This procedure will allow the Diamond II system to remain functional until the conversion of the final Diamond II ACU is completed.
7. Operational testing, staff training, and certification will be completed before system acceptance.

A.9 Additional Scope of Work Details

1. ACS: If required OCC, will provide any ACS server computers that may be required (contractor to determine if necessary. The master ACS control and recording server/appliance software will be installed by the Contractor at OCC's NOC on the Ballroom Level. ACS system administrator clients will be installed on designated workstations provided by OCC.
2. One (1) ACS ID badge station software client with a new ID badge printer will be installed at "Guest Services Office" on OCC's Intermediate/MLK Lobby Level.

3. Contractor will provide an initial quantity of 1000 HID iCLASS SE Model 300 printable access control cards.
4. VMS: The existing OnSSI VMS Base server is installed at OCC's NOC on the Ballroom Level. The current Ocularis IS license will be upgraded to an Ocularis LS license. MERC will provide the video recording computer servers.
5. All OCC Cameras will operate with an Ocularis LS camera license and will be recorded on the video servers provided by MERC. Contractor will provide the Ocularis software for the video recording servers.
6. Currently a single digital camera operating on the OnSSI VMS is in use at the OCC SOC. This camera is currently operating on an Ocularis IS channel license. This license will be upgraded to a LS channel license.
7. SOC: A new security console has been designed by Winsted (800.447.2257) for the OCC Security Operations Center. The design is registered under Winsted Quote Q34318305 131218 OCC 2014
8. Network: The ACS and VMS will utilize a dedicated OCC/Metro LAN established by the OCC/Metro's Information Systems Dept. OCC has sufficient fiber optic cable linking its IDF rooms with its NOC. OCC/Metro will provide ACS and VMS LAN switches (Standard and PoE) as required, equipment racks, high voltage power circuits, and UPS power supplies as required.
9. Contractor provides any high-lift required for cabling, camera mounts, ACS controller replacement, etc. as may be required for this project.

SYSTEM SPECIFICATION AND FUNCTION

B.1 Video Management (VMS) Specifications and Functions

The following outlines OCC VMS requirements. OCC currently utilizes the OnSSI Ocularis VMS. All existing and new camera control will be migrated to the existing OnSSI Ocularis VMS. Camera specifications by locations are provided in Attachment B. New cameras included are NC1, NC2, NC3, NC4, NC5, NC6, NC7, NC8, NC10, NC11, NC13, NC14, NC15, NC16, NC17, NC18, NC19, NC20, NC21, NC22, NC23, NC24, NC25, NC26, NC27, NC28, NC29, NC30, NC31, NC32, NC33, NC34, NC35, NC26, NC37, NC38, and NC39.

Products

1. The existing VMS system at OCC is an OnSSI Ocularis "IS" VMS. This VMS will be upgraded to the Ocularis "LS" Base server license. All cameras at OCC will operate under an Ocularis "LS" channel license. OnSSI offers a proven off-the-shelf API with most leading ACS. The OCC VMS system shall remain an OnSSI VMS System.
2. The Ocularis VMS will require an Ocularis compatible joystick controller with a camera selection feature. The OCC joystick controller shall be a VM Desktop USB Multifunction controller form CH Products (www.chproducts.com) Part Number 100-590,.
3. The four (4) 46" LED Video Monitors required for the SOC will be provided by contractor. These monitors shall be 24/7 operation Sony FWD-46B2 LED monitors.
4. The VMS video recording servers will be provided by MERC.
5. As referenced in the OCC Camera Requirements Document for the specific location/application listed, new IP Network cameras shall be the following camera models.
   a) Sony SNC-EP 550 with a 1MP 340° PTZ w/28x zoom with UNI WMB3 Low Profile Pendant Mount and UNI-INL7C2 enclosure.

b) Sony SNC-ER 550 with a 1MP 360° PTZ w/28x zoom. Pendant Mount and UNI-INL7C2 enclosure.
c) Sony SNC-EM602R 1.3MP dome with Infrared Illumination
d) Sony SNC-EM632R 3MP dome with Infrared Illumination
e) Sony SNC-VM631 3MP dome with ultra wide dynamic Visibility Enhancer
f) Axis P3354 Wide Angle Day/Nigh 1MP Dome camera
g) Axis M 3006 V 2mm Wide Angle Lens Dome

6. H.264 Video Encoders will be required to convert 64 analog cameras to digital. Since many of OCC's analog cameras are PTZ, the H.264 Encoders shall be a rack mounted in one (1) 1U and one (1) 3U Sony SNT EX Series Chassis's with sixteen (16) SNT-EX154/4CH Blade Enclosures offering H.264/MPEG4/JPEG. PTZ/AUDIO/ALARM with DEPA Advanced Intelligent Video.

7. Where existing coax video cable can be reutilized for IP cameras, a high speed Ethernet over Coax converter will be utilized. Converters will be Veracity High Wire.

General Requirements

1. All new interior and exterior cameras shall be PoE IP Network Cameras.
2. All new cameras will be UL listed with the appropriate label on the camera body.
3. All new exterior cameras (should they be required) will have appropriate surge protection against lightning strikes.
4. All video equipment will be installed per manufacturer's specifications.
5. Where test standards exist, all materials and products furnished by the contractor for construction shall bear the label of the Underwriters Laboratories (UL). All material, products, and components furnished by the contractor shall be manufactured, assembled, installed, and tested in accordance with the current industry standards.
6. All equipment and materials listed above shall be provided by the security contractor unless noted otherwise.
7. Contractor will provide up to 4 hrs of VMS system user training for system administrators.

Quality Assurance

All installation, configuration and setup of software as well as related work hereto shall by carried out by qualified technicians thoroughly trained and certified by OnSSI for the level of VMS to be installed and serviced at OCC.

B.2 Access control (ACS) Specification and Function

This section outlines the specifications for the Access Control System and related equipment as referenced on the drawings. The following specifications are meant to provide a baseline of features that OCC will require.

Products

1. The ACS system shall be a web-based system utilizing server appliances and Mercury controllers. The ACS must have an established API with the VMS. The ACS system shall be an S2 NETBOX Extreme S2-EXT-32-RM Controller System (with initial capacity for 32 card readers).
2. Card Readers will be HID iClass SE (RP10, RP40, RPK40).
3. Card credentials will be HID iClass SE printable ISO cards, Model 300.
4. All ACS reader controllers will have a power supplies with a minimum of 1 hr of backup battery protection. Power supplies will be Altronix.

5. All ACS reader controllers will have circuit surge protection.
6. The ACS Badge Station Printer shall be a dual sided ID ISO-30 badge printer. The ID Badge printer shall be a Magicard Rio Pro.
7. The ACS Badge Station ID Photo Camera shall be an 8 MP camera or better with Twain Driver TransTech Trans Cam Solo.
8. Contractor will provide up to 8 hrs of ACS system user training for system administrators and service personnel.

General Requirements

1. ACS System Specifications for the system replacing the existing Diamond II ACS are found in Attachment E.
2. Contractor will refer to security concept drawings provided on plan set at walkthrough for locations of current Diamond II card readers. All existing card reader locations will be controlled by the new ACS.
3. Contractor will refer to the Diamond II Panel Schedule in the Attachment C. All monitoring and control functions currently provided by the Diamond II ACS will be replicated by the new ACS.

Quality Assurance

All installation, configuration and setup of software as well as related work hereto shall by carried out by qualified technicians thoroughly trained and certified by the ACS Manufacturer for the level of ACS to be installed and serviced at OCC.

B.3 Security Operations Center (SOC) Specifications and Functions

The following outlines the equipment as referenced in the concept drawings. Refer to the equipment locations as referenced in the concept drawings.

Products

1. The existing SOC security console will be replaced with a console designed by Winsted (800.447.2257) under Winsted Quote Q34318305 131218 OCC 2014
2. The OCC joystick controller for the SOC shall be a VM Desktop USB Multifunction controller form CH Products (www.chproducts.com) Part Number 100-590
3. The 46” LCD Monitors for the SOC will be Sony FWD 46B2 HD LED Backlit Displays supplied by Contractor.

General Requirements

Contractor shall provide continuous coordination with OCC Security and minimize any delays and/or disruptions with the SOC during the construction period.

Quality Assurance

Contractor shall ensure that the new console and wall mounted display monitors are installed as per manufacturer’s recommendations.

SYSTEM ACCEPTANCE AND ADDITIONAL CONDITIONS

The purpose of this section is to provide the Contractor with information regarding the system acceptance process and requirements.

C.1 Performance, Testing, and Material Standards

Applicable code and standards bodies to be considered at a minimum.

i) The American National Standards Institute (ANSI)
ii) The Institute of Electrical and Electronic Engineers (IEEE)
iii) The National Electrical Code (NEC)
iv) Any Local Electrical Code(s).
v) The American Disabilities Act (ADA).
vi) Where other local standards supersede the aforementioned group. The contractor shall submit in writing the applicable standard replaced, and the new standard used.

C.2 Acceptance Process

The Contractor shall demonstrate that installation fulfills all requirements of the contract documents.

C.3 Design Changes and Substitutions

Design changes proposed by Contractor that affect the technical, dimensional, performance, or other requirements included in the drawings or plans initially approved by MERC shall not be made by Contractor without the prior written authorization of the MERC.

C.4 Rights to Documentation

All tangible materials delivered to MERC in connection with the work, including without limitation all drawings, schematics, flow charts, and other documentation prepared for MERC pursuant to this contract, shall belong to MERC. MERC reserves the right to reproduce and use any and all drawings, prints, or other data received from the Contractor which are considered necessary for engineering, operations, maintenance, or other MERC internal purposes related to the work despite any notice to the contrary appearing on the documents.

3. Deliverables/Outcomes

- **Work shall reach substantial completion by April 30, 2015**
- **Integrated VMS and ACS security system**
- **New Security Operations Center**
- **Conversion of 73 existing cameras to digital signal, per plans and specs.**
- **Furnish and installation of 37 new PoE cameras per plans and specs**

OCC Security Camera Requirements for Existing Cameras to be Repaired, Refocused, or Upgraded.

Note: All cameras replaced with Digital will require an OnSSI "LS" channel license with "Current" pro-rated to 2/7/2015

Drawing #	Service Camera	EXISTING Camera #	Location	Camera Type	Resolution	Mount	Remarks including FOV, IR, Mounting Heights, etc.	Placement Photo	To IDF #	Add Cam	Camera Action	New Cable
EXHIBIT LEVEL ES2.0	SC 1	1	Kitchen Corridor S	Fixed	Analog	Wall Mt	Inop--Replace w Sony SNC EM632R 3MP dome with IR	click	IDF 2		**REPLACE**	New Cat 6 50 ft
EXHIBIT LEVEL ES2.0		2	Kitchen Corridor N	Fixed	Analog							
EXHIBIT LEVEL ES2.0		3	Pre-function C	PTZ	Analog							
EXHIBIT LEVEL ES2.0		4	Pre-function A	PTZ	Analog							
EXHIBIT LEVEL ES2.0		5	Aramark Exterior Loading North Dock	PTZ	Analog					FALSE		
BALLROOM LEVEL ES 4.0	SC 2	6	Hall C	PTZ	Analog		Lens is blurred. Focus				**CLEAN**	
BALLROOM LEVEL ES 4.0		7	Hall C1	PTZ	Analog							
BALLROOM LEVEL ES 4.0		8	Exhibit Hall B	PTZ	Analog							
BALLROOM LEVEL ES 4.0		9	Hall A1	PTZ	Analog							
BALLROOM LEVEL ES 4.0		10	Hall A1	PTZ	Analog							
EXHIBIT LEVEL ES2.0	SC 3	11	Operations Exit in Corridor between A1 & Loading Dock	Fixed	Analog		blurred. Needs to be focused				**FOCUS**	
EXHIBIT LEVEL ES2.0		12	Exhibit B Loading Dock	PTZ	Analog							
BALLROOM LEVEL ES 4.0		13	1st Street & Oregon External	PTZ	Analog							
EXHIBIT LEVEL ES2.0		14	Loading Dock Service corridor behind D&E	fixed	Analog							
EXHIBIT LEVEL ES2.0		15	W Loading Dock South	PTZ	Analog							
EXHIBIT LEVEL ES2.0		16	W side fixed look I-5	Fixed	Analog							
BALLROOM LEVEL ES 4.0	SC 4	17	Exterior Ballroom North Plaza	PTZ	Analog		Relocate PTZ to view outer walkway				**REPOSITION**	
BALLROOM LEVEL ES 4.0	SC 5	18	MLK Lobby N	Fixed	3MP	Wall Mt	R&R PTZ w Sony SNC SNC VM631 3MP dome WDR	click	IDF 5		**REPLACE**	Use Existing Coax w/Highwire
BALLROOM LEVEL ES 4.0		19	Oregon Ballroom Lobby South	Fixed	Analog							
BALLROOM LEVEL ES 4.0		20	Oregon Ballroom Lobby North	Fixed	Analog							
BALLROOM LEVEL ES 4.0	SC-6	21	Holliday N Lobby	Fixed	Analog		Re point to view escalators				**REPOSITION**	
BALLROOM LEVEL ES 4.0		22	Bldg Exterior NW Corner 1st & Holliday	PTZ	Analog							
BALLROOM LEVEL ES 4.0		23	Bldg Exterior North Holliday Plaza Bell	PTZ	Analog							
EXHIBIT LEVEL ES2.0		24	SW Corner Lobby looking at S Parking	PTZ	Analog							
EXHIBIT LEVEL ES2.0		25	Management Room D Service Corridor	Fixed	Analog							
EXHIBIT LEVEL ES2.0	SC 7	26	Service Corridor Cocina Restaurant	Fixed	Analog		Raise up lens for better view				**REPOSITION**	
EXHIBIT LEVEL ES2.0	SC 8	27	Management Room B & C Service Corridor	Fixed	Analog	Wall Mt	Replace w Sony SNC EM632R 3MP dome with IR	click	IDF 2		**REPLACE**	New CAT 6 60ft
EXHIBIT LEVEL ES2.0	SC 9	28	Management Room A& B Service corridor	Fixed	Analog	Wall Mt	Replace w Sony SNC EM632R 3MP dome with IR	click	IDF 4		**REPLACE**	New CAT 6 60ft
P1 & P2 Parking Level ES1.0	SC 10	29	P2 south elevator lobby	Fixed	Analog		Reposition or may need wider lens				**REPOSITION**	
P1 & P2 Parking Level ES1.0		30	P1 South Elevator Lobby	Fixed	Analog							
P1 & P2 Parking Level ES1.0	SC 11	31	P1 East Elevator Lobby	Fixed	Analog		Reposition or may need wider Lens				**REPOSITION**	
P1 & P2 Parking Level ES1.0		32	P2 East Elevator Lobby	Fixed	Analog							
EXHIBIT LEVEL ES2.0	SC 12	33	Ginko Lobby South	PTZ	Analog		Video but no PTZ control Repair or replace with PTZ #18 MLK Lobby				**REPAIR**	
EXHIBIT LEVEL ES2.0	SC 13	34	F Lobby near meeting rooms F on SE corner	Fixed	Analog	Wall Mt	Inop--Replace w Sony SNC EM632R 3MP dome with IR	click	IDF B1		**REPLACE**	New CAT 6 80ft
EXHIBIT LEVEL ES2.0		35	F Lobby near meeting rooms F on SE corner	Fixed	Analog							
EXHIBIT LEVEL ES2.0		36	Mgt Room D corridor Elevator 15	Fixed	Analog							
EXHIBIT LEVEL ES2.0		37	Mgt Room D& E Service Corridor	Fixed	Analog							
EXHIBIT LEVEL ES2.0		38	Mgt Room C Service Corridor	Fixed	Analog							
EXHIBIT LEVEL ES2.0		39	Mgt Room A Service Corridor	Fixed	Analog							

OCC Security Camera Requirements for Existing Cameras to be Repaired, Refocused, or Upgraded.

Note: All cameras replaced with Digital will require an OnSSI "LS" channel license with "Current" pro-rated to 2/7/2015

Drawing #	Service Camera	EXISTING Camera #	Location	Camera Type	Resolution	Mount	Remarks including FOV, IR, Mounting Heights, etc.	Placement Photo	To IDF #	Add Cam	Camera Action	New Cable
EXHIBIT LEVEL ES2.0		40	1st floor Elevator # 13 & 14 at Ginko Lobby	Fixed	Analog				☐			
P1 & P2 Parking Level ES1.0		41	P1 Entry on South side	PTZ	Analog				☐			
P1 & P2 Parking Level ES1.0		42	P1 Entry on South side	Fixed	Analog				☐			
P1 & P2 Parking Level ES1.0		43	P1 Stairway	Fixed	Analog				☐			
P1 & P2 Parking Level ES1.0		44	P2 Entrance	PTZ	Analog				☐			
P1 & P2 Parking Level ES1.0		45	P2 Entrance	Fixed	Analog				☐			
P1 & P2 Parking Level ES1.0		46	P2 man door entry	Fixed	Analog				☐			
BALLROOM LEVEL ES 4.0		47	Bldg Exterior West Loading Dock South	PTZ	Analog				☐			
EXHIBIT LEVEL ES2.0		48	Hall E Service Corridor	Fixed	Analog		This camera is now mounted near ceiling cable tray viewing the exit		☐			
EXHIBIT LEVEL ES2.0		49	Loading Dock interior North side of old docks	PTZ	Analog				☐			
BALLROOM LEVEL ES 4.0	SC 14	50	Hall E SW	PTZ	Analog		Reposition Camera		☑		**REPOSITION**	
BALLROOM LEVEL ES 4.0		51	City View Elevator 18 in service corridor North at Ginko	Fixed	Analog				☐			
BALLROOM LEVEL ES 4.0	SC 15	52	Service Corridor South of Hall E	Fixed	Analog		Adjust camera slightly 10 degrees left.		☑		**REPOSITION**	
BALLROOM LEVEL ES 4.0	SC 16	53	MLK Lobby S	PTZ	Analog	Ceiling Mt	R&R w/SNC-EP550, 1MP 340° PTZ w/28x, UNI WMB3 & UNI-INL7C2	click	IDF 5 ☑		**REPLACE**	Use Existing Coax w/Highwire
EXHIBIT LEVEL ES2.0		54	Exhibitors' entrance by Security Office	Fixed	Analog				☐			
EXHIBIT LEVEL ES2.0		55	Inside Security Office Lobby	Fixed	Analog				☐			
BALLROOM LEVEL ES 4.0		56	Hall D1 west NW	PTZ	Analog				☐			
BALLROOM LEVEL ES 4.0	SC 17	57	West Loading Dock	PTZ	Analog		Needs cleaning		☑		**CLEAN**	
BALLROOM LEVEL ES 4.0		58	Exhibit Hall D	PTZ	Analog				☐			
BALLROOM LEVEL ES 4.0	SC 18	59	North Side of Ginko Lobby	PTZ	Analog		Lower 1 or 2". Some blooming. Reposition to Ballroom entries		☑		**REPOSITION**	
Intermediate level ES3.0	SC 19	60	Money Room	Fixed	Analog	Ceiling Mt	Replace with Sony SNC EM602R 1.3MP dome with IR		IDF 5 ☑		**REPLACE**	Use Existing Coax w/Highwire
BALLROOM LEVEL ES 4.0		61	Portland Ballroom Lobby near 251	PTZ	Analog				☐			
BALLROOM LEVEL ES 4.0	SC 20	62	Portland Ballroom Lobby	Fixed	Analog		Reposition Camera		☑		**REPOSITION**	
BALLROOM LEVEL ES 4.0		63	Portland Ballroom Corridor South	Fixed	Analog				☐			
BALLROOM LEVEL ES 4.0		64					No camera. This camera was removed		☐		No Action	
BALLROOM LEVEL ES 4.0		65	Bldg Exterior MLK Portland Ballroom East	PTZ	Analog				☐			
BALLROOM LEVEL ES 4.0		66	Bldg Exterior MLK & Lloyd	PTZ	Analog				☐			
BALLROOM LEVEL ES 4.0		67	Bldg Exterior South over P1 Entrance	PTZ	Analog				☐			
BALLROOM LEVEL ES 4.0	SC 21	68	Inside Holliday North Lobby	PTZ	Analog		Out of Focus, some blurry, some blooming		☑			
EXHIBIT LEVEL ES2.0	SC 22	69	Inside Aramark Shipping & Receiving North Loading Dock.	Fixed	Analog		Remove Existing Camera 69	click	☑		**REMOVE**	
EXHIBIT LEVEL ES2.0	SC 23	70	Inside North Loading Dock. Aramark	Fixed	Analog	Wall Mt	Replace & relocate w/Sony SNC EM632R 3MP dome w IR	click	IDF 5 ☑		**REPLACE**	CAT 6 60'
BALLROOM LEVEL ES 4.0		71	Portland Ballroom Lobby Elevator 16 & 17	Fixed	Analog		Camera is bit tilted.		☐			
BALLROOM LEVEL ES 4.0		72	Business Ctr	Fixed	Analog				☐			
P1 & P2 Parking Level ES1.0		73	P2 Parking Office	Fixed	Analog				☐			
BALLROOM LEVEL ES 4.0		74	King Lobby Ticket Office	Fixed	Analog				☐			
BALLROOM LEVEL ES 4.0	SC 24	75	Network Cam to OCC Plaza	PTZ	Digital		Provide LS Camera License with "Current" Pro-Rated to 2/7/2015		☑		**Add ONSSI License**	

OCC Security Camera Requirements: New & Optional Cameras to Added

New Cameras to be added to VMS system are listed below

Note: All New cameras added will require an OnSSI "LS" channel license with "Current" pro-rated to 2/7/2015

Drawing	New Camera Additions	From IDF	Location	Camera Type	Resolution	Mount	Camera Recommendation	Placement Photo		Add Cam	Optional Camera #	Cameras Added	Cabling Comments	Approx CAT 6 Cable Distance
EXHIBIT LEVEL ES2.0	NC 1	IDF-E1	Inside Loading Dock at D	PTZ	1MP	Ceiling Mt	Sony SNC-EP 550 1MP 340° PTZ w/28x, UNI WMB3 & UNI-INL7C2 enclosure.	click	☑			1	IDF E1 routed thru cable tray; mount on cable tray support or pipe rack for easiest access	70'
EXHIBIT LEVEL ES2.0	NC 2	IDF-5	Aramark --Add camera to above dock entry door	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑		Option #1	1	IDF 5 to Camera. Short run	50'
EXHIBIT LEVEL ES2.0	NC 3	IDF-5	Aramark-Add camera to N Dock in Trash Compactor	Fixed	3MP	Wall Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	#REF!	☑		Option #2	1	IDF 5 to Camera. Short run	50'
EXHIBIT LEVEL ES2.0	NC4	iDF-4	Aramark Add cam to Entry to Money Rm	Fixed	3MP	Wall Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	#REF!	☑		Option #3	1	IDF 4 to Camera. Down hall & into Money Room	40'
EXHIBIT LEVEL ES2.0	NC 5	IDF-4	Aramark--Kitchen Corridor at North Stairway Exit	Fixed	3MP	Wall Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑		Option #4	1	IDF 4 to Camera . Down Hallway	30'
EXHIBIT LEVEL ES2.0	NC 6	IDF 4	Pre-Function A to view Escalators	Fixed	3MP	Ceiling Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑			1	IDF 4, difficult long run thru A/B meeting rooms. Opt 1: route straight across A103-104, svc corr., & A105. Opt 2: pipe to AB svc corridor & down corridor to cable tray. Repeater?	Opt 1: 140' Opt 2: 340'
EXHIBIT LEVEL ES2.0	NC 7	IDF 4	Aramark at Kitchen Storeroom at Rollup	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑		Option #5	1	IDF 4 to Camera. Down Hallway	40'
EXHIBIT LEVEL ES2.0	NC 8	IDF 4	Aramark Corridor to Mtng Rms A-B-C at A&B	Fixed	3MP	Ceiling Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑		Option #6	1	IDF 4 to Camera. Down hallway	110'
									☐					
EXHIBIT LEVEL ES2.0	NC 10	IDF 2	Aramark-South Wall west side to View Kitchen	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑		Option #8	1	IDF2 to Camera. Down hall & into kitchen	170'
EXHIBIT LEVEL ES2.0	NC 11	IDF 2	Aramark-Kitchen South ceiling at cooler	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑		Option #9	1	IDF2 to Camera. Down hall & into kitchen	180'
									☐					
EXHIBIT LEVEL ES2.0	NC 13	IDF 2	Aramark-Add camera to view restroom corridor	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑		Option #11	1	IDF2 to Camera. Down hall & into kitchen	180'
EXHIBIT LEVEL ES2.0	NC 14	IDF 2	Aramark-Add camera to south wall. View Dishwash	Fixed	3MP	Ceiling Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑		Option #12	1	IDF2 to Camera. Down hall & into Dish room	55'
EXHIBIT LEVEL ES2.0	NC 15	IDF 2	Aramark-Add camera near closet viewing Prep Area	Fixed	3MP	Ceiling Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑		Option #13	1	IDF2 to Camera in hallway	40'
EXHIBIT LEVEL ES2.0	NC 16	IDF 2	Pre-Function C to view escalators	Fixed	3MP	Ceiling Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑			1	IDF 2, difficult long run thru B/C meeting rooms. Opt 1: route straight across C126-125, svc corr., & C124. Opt 2: pipe to BC svc corridor & down corridor to cable tray. Repeater?	Opt 1: 140' Opt 2: 340'
EXHIBIT LEVEL ES2.0	NC 17	IDF C1	East Side C-D Service Corridor Center	Fixed	1.3MP	Ceiling Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑			1	C1, route to cable tray	90'
EXHIBIT LEVEL ES2.0	NC 18	IDF B1	Ginko Lobby	Fixed	3MP	Ceiling Mt	Sony SNC VM631 3MP dome with ultra wide dynamic	click	☑			1	B1, run in cable tray	200'
EXHIBIT LEVEL ES2.0	NC 19	IDF A1	Aramark-Add Camera to view Coffee Prep Station	Fixed	1.3MP	Ceiling Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑		Option #14	1	IDF A1 to camera. Down hallway to Coffee Prep	60'
EXHIBIT LEVEL ES2.0	NC 20	IDF B1	New Cam to view D&E Entrances	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑			1	B1, run in cable tray. Repeater needed?	320'
EXHIBIT LEVEL ES2.0	NC 21	IDF D1	Public Corridor (South of Exhibit E)	Fixed	1.3MP	Ceiling Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑			1	D1, new conduit to service corridor to cable tray; surface mount on wall above door to avoid hard ceiling in public corridor	250'
Intermediate level ES3.0	NC 22	IDF 1	Guest Services	Fixed	1MP	Ceiling Mt	Axis P3354 Indoor 1MP Dome camera	click	☑			1	Opt. 1: IDF 1, existing conduits in Guest Sacs. Lobby. Opt. 2: IDF C1-follow existing station wiring to cable tray below.	Opt 1: 100' Opt. 2: 250'
Intermediate level ES3.0	NC 23	IDF 7	Aramark Add discreet Camera to STIX storeroom	Fixed	1MP	Wall Mt	AXIS M3006-V Wide Angle Lens 1 MP	click	☑		Option #15	1	IDF 7 to camera. Very short run inside same area	30'
BALLROOM LEVEL ES 4.0	NC 24	IDF G3	Portland Ballroom Public Corridor South at Exit	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑			1	Opt. 1: G3 move camera to lobby side, facing toward svc corr. Pipe across lobby ceiling up into void & around to IDF. Opt 2: D1 penetrate floor into corridor below & join run for NC21.	Opt 1: 270' Opt 2: 270'
BALLROOM LEVEL ES 4.0	NC 25	IDF F3	Aramark-cam in Plating kitchen to view elevator	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑		Option #16	1	IDF F3, run thru vacant space, or pipe across lobby into the side of IDF right above the stairs.	180
BALLROOM LEVEL ES 4.0	NC 26	IDF F3	Portland Ballroom Public Corridor N Corridor at Elevators	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑			1	IDF F3, run thru vacant space, or pipe across lobby into the side of IDF right above the stairs.	180'
BALLROOM LEVEL ES 4.0	NC 27	IDF C1	Inside Admin Office	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑			1	IDF C1 Opt 1: route thru ceiling to conduit down to cable tray Opt 2: open wall behind receptionist & penetrate floor down to svc corridor, then to cable tray	Opt 1: 130' Opt 2: 110'
BALLROOM LEVEL ES 4.0	NC 28	IDF 2	MLK Electronic Sign--1st camera views south.	Fixed	3MP	Sign Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑			1	IDF 2, existing conduit.	100'
BALLROOM LEVEL ES 4.0	NC 29	IDF 2	MLK Electronic Sign--2nd camera views north	Fixed	3MP	Sign Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑			1	IDF 2, existing conduit.	100'
BALLROOM LEVEL ES 4.0	NC 30	IDF 4	Holladay Electronic Sign. Views west to Holladay entry	Fixed	3MP	Sign Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑			1	IDF 4, existing conduit.	60'
BALLROOM LEVEL ES 4.0	NC 31	IDF 4	Holladay Electronic Sign. Views east to MLK Blvd.	Fixed	3MP	Sign Mt	Sony SNC EM632R 3MP dome with Infrared Illumination	click	☑			1	IDF 4, existing conduit.	60'
BALLROOM LEVEL ES 4.0	NC 32	IDF 10	Oregon Ballroom Lobby near North Round	Fixed	3MP	Ceiling Mt	Sony SNC VM631 3MP dome with ultra wide dynamic	click	☑			1	IDF 10, across lobby down corridor	160'
BALLROOM LEVEL ES 4.0	NC 33	IDF 10	Oregon Ballroom North Entrance	Fixed	3MP	Ceiling Mt	Sony SNC VM631 3MP dome with ultra wide dynamic	click	☑			1	Opt. 1: IDF 10 through ballroom and/or stairwell & down svc corr. Opt. 2: IDF 04: place camera at rotunda kiosk & use existing path	200'
BALLROOM LEVEL ES 4.0	NC 34	IDF 2	Oregon Ballroom South Entrance	Fixed	3MP	Ceiling Mt	Sony SNC VM631 3MP dome with ultra wide dynamic	click	☑			1	Opt. 1: IDF 9 through ballroom and/or stairwell & down svc corr. Opt. 2: IDF 02: place camera at rotunda kiosk & use existing path	200'

OCC Security Camera Requirements: New & Optional Cameras to Added

New Cameras to be added to VMS system are listed below

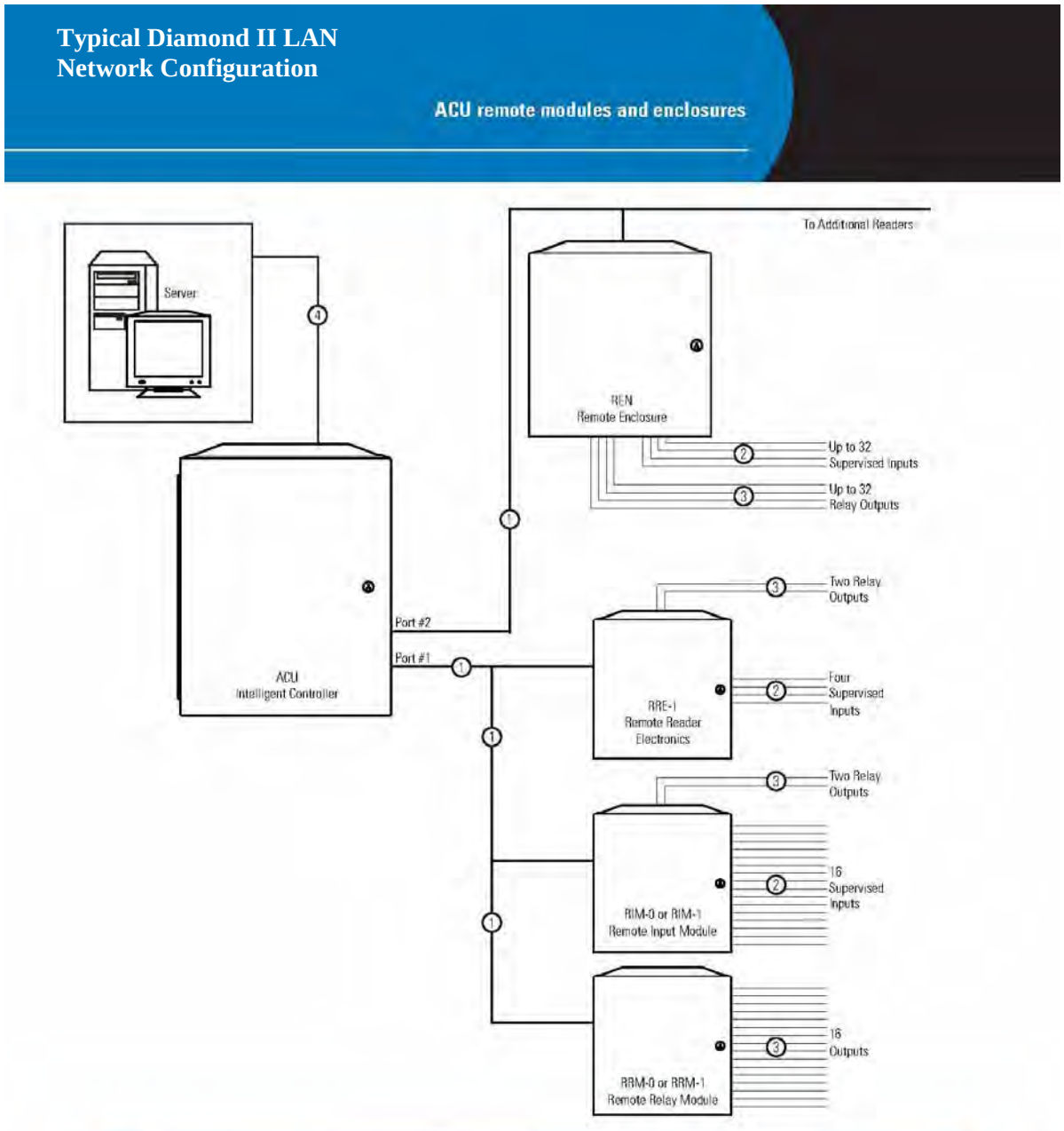
Note: All New cameras added will require an OnSSI "LS" channel license with "Current" pro-rated to 2/7/2015

Drawing	New Camera Additions	From IDF	Location	Camera Type	Resolution	Mount	Camera Recommendation	Placement Photo		Add Cam	Optional Camera #	Cameras Added	Cabling Comments	Approx CAT 6 Cable Distance
BALLROOM LEVEL ES 4.0	NC 35	IDF 9	Oregon Ballroom Lobby near East Round	Fixed	3MP	Ceiling Mt	Sony SNC VM631 3MP dome with ultra wide dynamic	click	☑			1	IDF 9, across lobby down corridor	160'
BALLROOM LEVEL ES 4.0	NC 36	IDF 1	MLK Lobby to view lobby from above elevators	Fixed	3MP	Wall Mt	Sony SNC VM631 3MP dome with ultra wide dynamic	click	☑			1	IDF 1, existing conduits in Guest Svcs. Lobby ??, OR vertical through VIC area - pipe through existing floor holes poured for HVAC & sprinklers	100'-150'
BALLROOM LEVEL ES 4.0	NC 37	IDF 3	Relocated at VIP Suite B	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☐			0	IDF 3 - Pipe into corridor & out to Hall B AV balcony; straight down to IDF	80'
BALLROOM LEVEL ES 4.0	NC 38	IDF 3	Relocated at VIP Suite B	Fixed	1.3MP	Wall Mt	Sony SNC EM602R 1.3MP dome with Infrared Illumination	click	☑			1	IDF 3, run thru VIP B ceiling & join run for NC37	150'
BALLROOM LEVEL ES 4.0	NC 39	IDF 5	Holliday N Lobby to view lobby from above elevators	Fixed	3MP	Wall Mt	Sony SNC VM631 3MP dome with ultra wide dynamic	click	☑			1	IDF 5, thru mech space, vertical through Show Mgr office/pacificwild storage area	100'

Note #1: Sony Gen 5 camera models are changed to their Gen 6 equivalent (SNC-DH160 to SNC-EM602R, SNC-DH260 to SNC-EM632R, SNC-DH240T to SNC-VM631)
Note #2: Sony PTZ Gen 5 models and Axis dome cameras may be upgraded by change order.
Note #3: Where provided, Column "I" provides a "click function" to view a "camera placement photo" in Sheet 2. After viewing photo, select Sheet 1 in the lower left of Sheet 2 to return to Sheet 1.

OCC's Existing Infographics Diamond II Access Control Panel Configuration

The purpose of the following ACU schedules & Network Diagram is to provide bidders will an overview of the existing OCC ACS panels, inputs & outputs, and card readers it controls for purposes of replication by a replacement ACS.



Cable #	Description	Belden Cable Number (or equal)	Max. Distance
1	Communication (RS-485)	#9842 or Alpha #6222C, 24 AWG, 2-pair, individual shields, braid overall shield	4,000' (1,220 m)
		And	
	Power (24 VDC)	#9409 or Alpha #1897C, 18 AWG, 2-conductor/unshielded	4,000' (1,220 m)
2	Supervised input	#9407 or Alpha #1172C, 22 AWG, 2-conductor/unshielded	1,000' (305 m)
3	Relay output	#9409 or Alpha #1897C, 18 AWG, 2-conductor/unshielded	1,000' (305 m)
4	Communication (RS-485)	#9842 or Alpha #6222C, 24 AWG, 2-pair, individual shields, braid overall shield	4,000' (1,220 m)

At OCC, there are a total 4 ACU's, 14 RIMs, 16 RREs, and 2 RRMs. Two of the RREs are installed next to the ACU-0 at the P2 Parking office, and the rest of the RIMs, RREs, & RRMs are installed near the doors they control or monitor. Each has a number of inputs, outputs, & relays detailed in the Diamond II Panel Schedule provided with this RFP. For purposes of the RFP, bidders will assume the existing ACS cabling & enclosures are reusable.

Diamond II ACU #0

ACU-0 is located in the P2 Parking Office

CONTROLLER PANEL SCHEDULE		ACU # 0	
PANEL LOCATION:			
	PARKING LEVEL 2071		
	INPUTS	START # 1	
ACU INPUT #	ACU INPUT LOCATION	POINT #	POINT NAME
1	ACU SUPERVISED INPUT #1	1	P2 ENTRY ROLL UP DC
2	ACU SUPERVISED INPUT #2	2	P2 ENTRY ROLL UP DC
3	ACU SUPERVISED INPUT #3	3	P-1074
4	ACU SUPERVISED INPUT #4	4	P-1073
5	ACU SUPERVISED INPUT #5	5	P-1000.3
6	ACU SUPERVISED INPUT #6	6	P-1000.2
7	ACU SUPERVISED INPUT #7	7	P-1000.1
8	ACU SUPERVISED INPUT #8	8	P-1003
9	ACU SUPERVISED INPUT #9	9	P-1002
10	ACU SUPERVISED INPUT #10	10	NOT USED
11	ACU SUPERVISED INPUT #11	11	NOT USED
12	ACU SUPERVISED INPUT #12	12	NOT USED
13	ACU SUPERVISED INPUT #13	13	NOT USED
14	ACU SUPERVISED INPUT #14	14	NOT USED
15	ACU SUPERVISED INPUT #15	15	NOT USED
16	ACU SUPERVISED INPUT #16	16	NOT USED
	CARD READERS	START # 0	
PORT# RRE#	RRE READER LOCATION	READER NUMBER	DOOR NAME
P2 RRE0	PARKING LEVEL 2 WEST	0	P2051
P2 RRE 1	PARKING LEVEL 2 WEST	1	P2073
P2 RRE2	PARKING LEVEL 2 WEST	2	P-2 ENTRY
P2 RRE3	PARKING LEVEL 2 WEST	3	P-1 ENTRY
P1 RRE0	PARKING LEVEL 2 EAST	4	P-2100
P1 RRE1	PARKING LEVEL 2 EAST	5	P-2030
P1 RRE2	PARKING LEVEL 1 EAST	6	P-1040
P1 RRE3	PARKING LEVEL 1 EAST	7	P-1140

Diamond II ACU #1

ACU-1 is located in IDF E1

CONTROLLER PANEL SCHEDULE		ACU # 1	
PANEL LOCATION:			
	T-1741		
	INPUTS	START #	1
ACU INPUT #	**ACU INPUT LOCATION**	**POINT #**	**POINT NAME**
1	ACU SUPERVISED INPUT #1	1	NOT USED
2	ACU SUPERVISED INPUT #2	2	NOT USED
3	ACU SUPERVISED INPUT #3	3	NOT USED
4	ACU SUPERVISED INPUT #4	4	NOT USED
5	ACU SUPERVISED INPUT #5	5	NOT USED
6	ACU SUPERVISED INPUT #6	6	NOT USED
7	ACU SUPERVISED INPUT #7	7	NOT USED
8	ACU SUPERVISED INPUT #8	8	NOT USED
9	ACU SUPERVISED INPUT #9	9	NOT USED
10	ACU SUPERVISED INPUT #10	10	NOT USED
11	ACU SUPERVISED INPUT #11	11	NOT USED
12	ACU SUPERVISED INPUT #12	12	NOT USED
13	ACU SUPERVISED INPUT #13	13	NOT USED
14	ACU SUPERVISED INPUT #14	14	NOT USED
15	ACU SUPERVISED INPUT #15	15	NOT USED
16	ACU SUPERVISED INPUT #16	16	NOT USED
	CARD READERS	START #	0
PORT# RRE#	**RRE READER LOCATION**	**READER NUMBER**	**DOOR NAME**
P2 RRE0	MAIN LEVEL SW	0	1760
P2 RRE 1	MAIN LEVEL SW	1	1761
P2 RRE2	MAIN LEVEL SW	2	1788
		3	
		4	
		5	
		6	
		7	
PORT# RIM#	**RIM INPUT MODULE LOCATION**	**RIM I/O NUMBER**	**INPUT NAME**
P1 RIM 4	MAIN LEVEL SW 1741	1	1781
		2	1782
		3	1783
		4	1784
		5	1785
		6	1786
		7	1787
		8	CD1
		9	CD2
		10	CD3
		11	CD4
		12	CD5
		13	CD6
		14	
		15	
		16	
		RIM OUTPUT 1	
		RIM OUTPUT 2	

Diamond II ACU #1 Continued

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM I/O NUMBER	INPUT NAME
P1 RIM 5	MAIN LEVEL SW 1660	1	1642
		2	1641
		3	1640
		4	CD14
		5	CD12
		6	CD11
		7	CD10
		8	CD9
		9	CD8
		10	CD7
		11	1711
		12	1821
		13	1822
		14	
		15	
		16	
		RIM OUTPUT 1	
		RIM OUTPUT 2	

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM INPUT NUMBER	INPUT NAME
P1 RIM 6	UPPER LEVEL SW IA2.23	1	3900
		2	3931
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	
		RIM OUTPUT 1	3900 LOCK OUTPUT
		RIM OUTPUT 2	3931 LOCK OUTPUT

PORT# RRM#	RRM OUTPUT MODULE LOCATION	RRM OUTPUT NUMBER	OUTPUT NAME
P2 RRM 4	MAIN LEVEL SW CD 1-6	1	CD 1
		2	CD 1
		3	CD 2
		4	CD 2
		5	CD 3
		6	CD 3
		7	CD 4
		8	CD 4
		9	CD 5
		10	CD 5
		11	CD 6
		12	CD 6
		13	
		14	
		15	
		16	

Diamond II ACU #1 Continued

PORT# RRM#	RRM OUTPUT MODULE LOCATION	RRM OUTPUT NUMBER	OUTPUT NAME
P2 RRM 5	MAIN LEVEL SW CD 7-12	1	CD 7
		2	CD 7
		3	CD 8
		4	CD 8
		5	CD 9
		6	CD 9
		7	CD 10
		8	CD 10
		9	CD 11
		10	CD 11
		11	CD 12
		12	CD 12
		13	
		14	
		15	
		16	

Diamond II ACU #2

ACU-2 is located in IDF C1

CONTROLLER PANEL SCHEDULE		ACU # 2	
PANEL LOCATION:			
	T-1852		
	INPUTS	START #	1
ACU INPUT #	ACU INPUT LOCATION	POINT #	POINT NAME
1	ACU SUPERVISED INPUT #1	1	3640 DA
2	ACU SUPERVISED INPUT #2	2	NOT USED
3	ACU SUPERVISED INPUT #3	3	NOT USED
4	ACU SUPERVISED INPUT #4	4	NOT USED
5	ACU SUPERVISED INPUT #5	5	NOT USED
6	ACU SUPERVISED INPUT #6	6	NOT USED
7	ACU SUPERVISED INPUT #7	7	NOT USED
8	ACU SUPERVISED INPUT #8	8	NOT USED
9	ACU SUPERVISED INPUT #9	9	NOT USED
10	ACU SUPERVISED INPUT #10	10	NOT USED
11	ACU SUPERVISED INPUT #11	11	NOT USED
12	ACU SUPERVISED INPUT #12	12	NOT USED
13	ACU SUPERVISED INPUT #13	13	NOT USED
14	ACU SUPERVISED INPUT #14	14	NOT USED
15	ACU SUPERVISED INPUT #15	15	NOT USED
16	ACU SUPERVISED INPUT #16	16	NOT USED
	CARD READERS	START #	0
PORT# RRE#	RRE READER LOCATION	READER NUMBER	DOOR NAME
P1 RRE0	MAIN LEVEL SE	0	1003 CONTROLS DOOR 1000-1002
		1	
		2	
		3	
		4	
		5	
		6	
		7	

Diamond II ACU #2 Continued

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM I/O NUMBER	INPUT NAME
P1 RIM 4	MAIN LEVEL SE T1181	1	1029-1031
		2	1032-1034
		3	1035-1037
		4	1038-1040
		5	1430
		6	1440
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM I/O NUMBER	INPUT NAME
P1 RIM 5	MAIN LEVEL SE T1220	1	1000
		2	1001
		3	1002
		4	1020-1022
		5	1023-1025
		6	1026-1028
		7	1250
		8	1260
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM INPUT NUMBER	INPUT NAME
P2 RIM 4	INTERMEDIATE LEVEL NE	1	2065 DA
		2	2011 DA
		3	2012 DA
		4	2000 A-F
		5	2000 G-I
		6	2000 U-L
		7	2000 M-L
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

Diamond II ACU #2 Continued

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM INPUT NUMBER	INPUT NAME
P2 RIM 5	UPPER LEVEL NE	1	3047A-3047C
		2	3047D-3047F
		3	3047G-3047L
		4	
		5	
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM INPUT NUMBER	INPUT NAME
P2 RIM 6	UPPER LEVEL NE	1	3041A-3041C
		2	3044A-3044C
		3	3044D-3044F
		4	3044G-3044I
		5	
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM INPUT NUMBER	INPUT NAME
P2 RIM 7	INTERMEDIATE LEVEL NW	1	2010-2010B
		2	2010C-2010H
		3	2010I-2010K
		4	2010L-2010N
		5	2010O-2010Q
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

Diamond II ACU #3

ACU-3 is located in IDF 5

CONTROLLER PANEL SCHEDULE		ACU # 3	
PANEL LOCATION:			
	T-1115		
	INPUTS	START #	1
ACU INPUT #	**ACU INPUT LOCATION**	**POINT #**	**POINT NAME**
1	ACU SUPERVISED INPUT #1	1	NOT USED
2	ACU SUPERVISED INPUT #2	2	NOT USED
3	ACU SUPERVISED INPUT #3	3	NOT USED
4	ACU SUPERVISED INPUT #4	4	NOT USED
5	ACU SUPERVISED INPUT #5	5	NOT USED
6	ACU SUPERVISED INPUT #6	6	NOT USED
7	ACU SUPERVISED INPUT #7	7	NOT USED
8	ACU SUPERVISED INPUT #8	8	NOT USED
9	ACU SUPERVISED INPUT #9	9	NOT USED
10	ACU SUPERVISED INPUT #10	10	NOT USED
11	ACU SUPERVISED INPUT #11	11	NOT USED
12	ACU SUPERVISED INPUT #12	12	NOT USED
13	ACU SUPERVISED INPUT #13	13	NOT USED
14	ACU SUPERVISED INPUT #14	14	NOT USED
15	ACU SUPERVISED INPUT #15	15	NOT USED
16	ACU SUPERVISED INPUT #16	16	NOT USED
	CARD READERS	START #	0
PORT# RRE#	**RRE READER LOCATION**	**READER NUMBER**	**DOOR NAME**
P1 RRE0	MAIN LEVEL NW	0	NW LOADING DOCK
P1 RRE1		1	WEST EMPLOYEE ENTRANCE
P1 RRE2		2	WEST EMPLOYEE GATE
P1 RRE3		3	WEST EMPLOYEE VEHICLE GATE
		4	
		5	
		6	
		7	
PORT# RIM#	**RIM INPUT MODULE LOCATION**	**RIM I/O NUMBER**	**INPUT NAME**
P1 RIM 4	MAIN LEVEL NW	1	1221 A-E
		2	1221 F-J
		3	CD 1221
		4	
		5	
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

Diamond II ACU #3 Continued

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM I/O NUMBER	INPUT NAME
P1 RIM 5	MAIN LEVEL NW	1	1216 D-F
		2	1217 A-B CD 1217
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM INPUT NUMBER	INPUT NAME
P1 RIM 6	MAIN LEVEL NW	1	CD 1194 B-P
		2	CD 1194 K
		3	1194 A1-B2
		4	
		5	
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

PORT# RIM#	RIM INPUT MODULE LOCATION	RIM INPUT NUMBER	INPUT NAME
P2 RIM 4	MAIN LEVEL NE	1	1132 A-E
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

Diamond II ACU #3 Continued

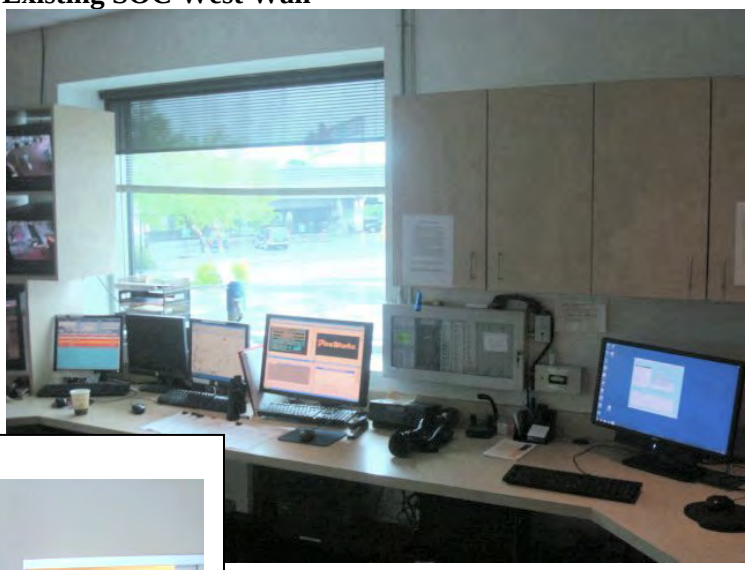
PORT# RIM#	RIM INPUT MODULE LOCATION	RIM INPUT NUMBER	INPUT NAME
P2 RIM 5	MAIN LEVEL NE	1	1153 B-G
		2	
		3	
		4	
		5	
		6	
		7	
		8	
		9	
		10	
		11	
		12	
		13	
		14	
		15	
		16	

Existing & Redesigned Security Operations Center

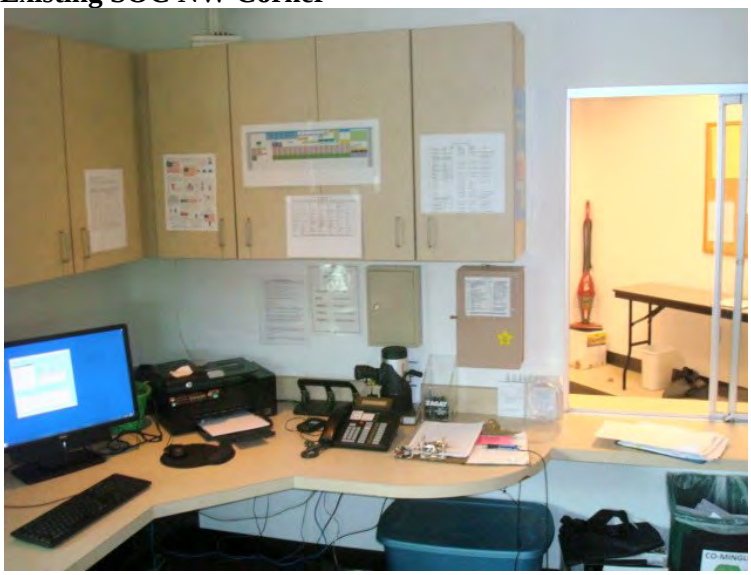
The following photos show the existing OCC SOC:

Existing SOC SW Corner

Existing SOC West Wall

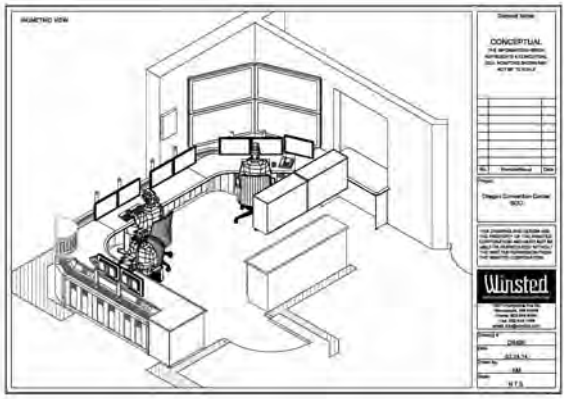


Existing SOC NW Corner

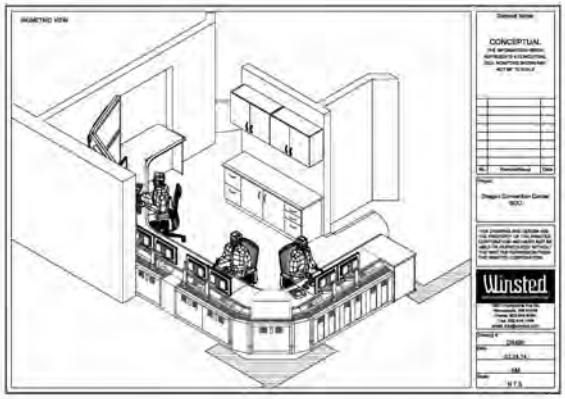


The following drawings depict the redesigned SOC with the new security console:

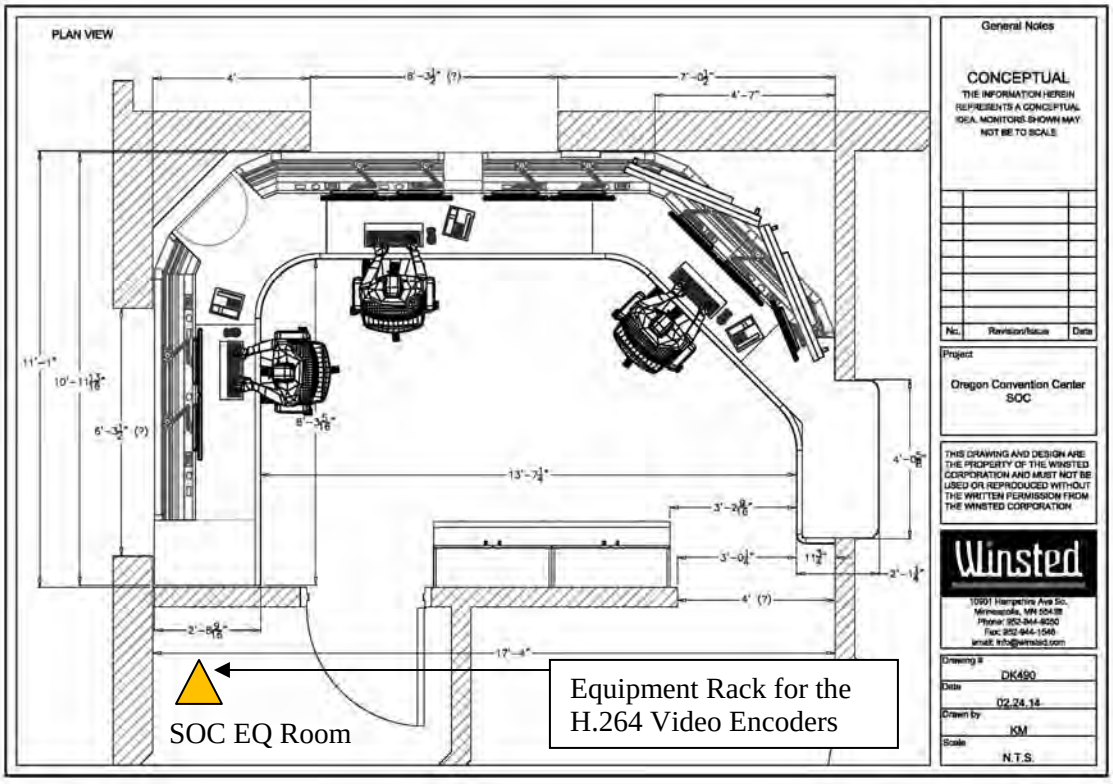
Redesigned SOC NW Corner View

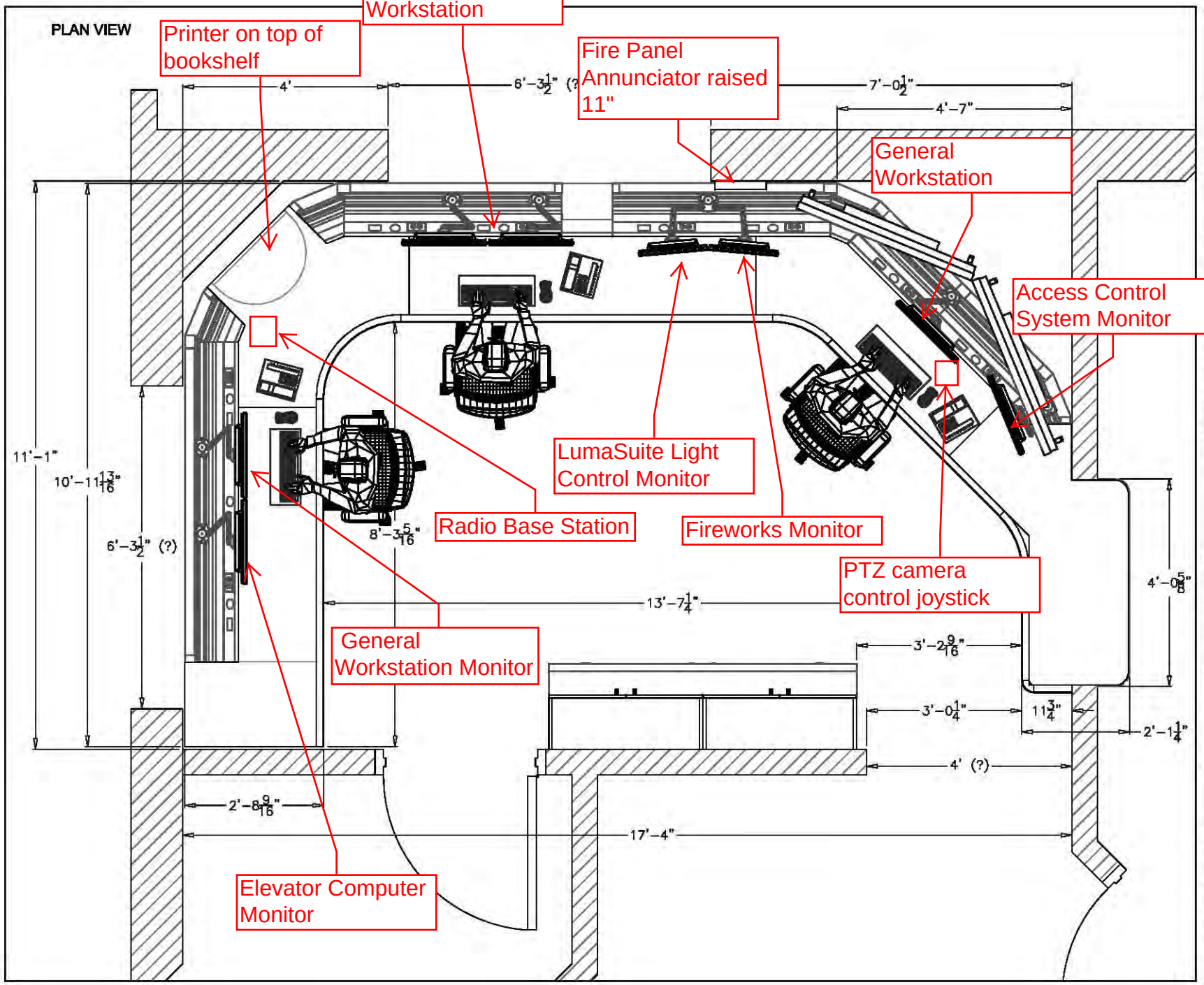


Redesigned SOC East Wall View



Upgraded SOC Floor Plan





General Notes

CONCEPTUAL

THE INFORMATION HEREIN REPRESENTS A CONCEPTUAL IDEA. MONITORS SHOWN MAY NOT BE TO SCALE.

No.	Revision/Issue	Date

Project

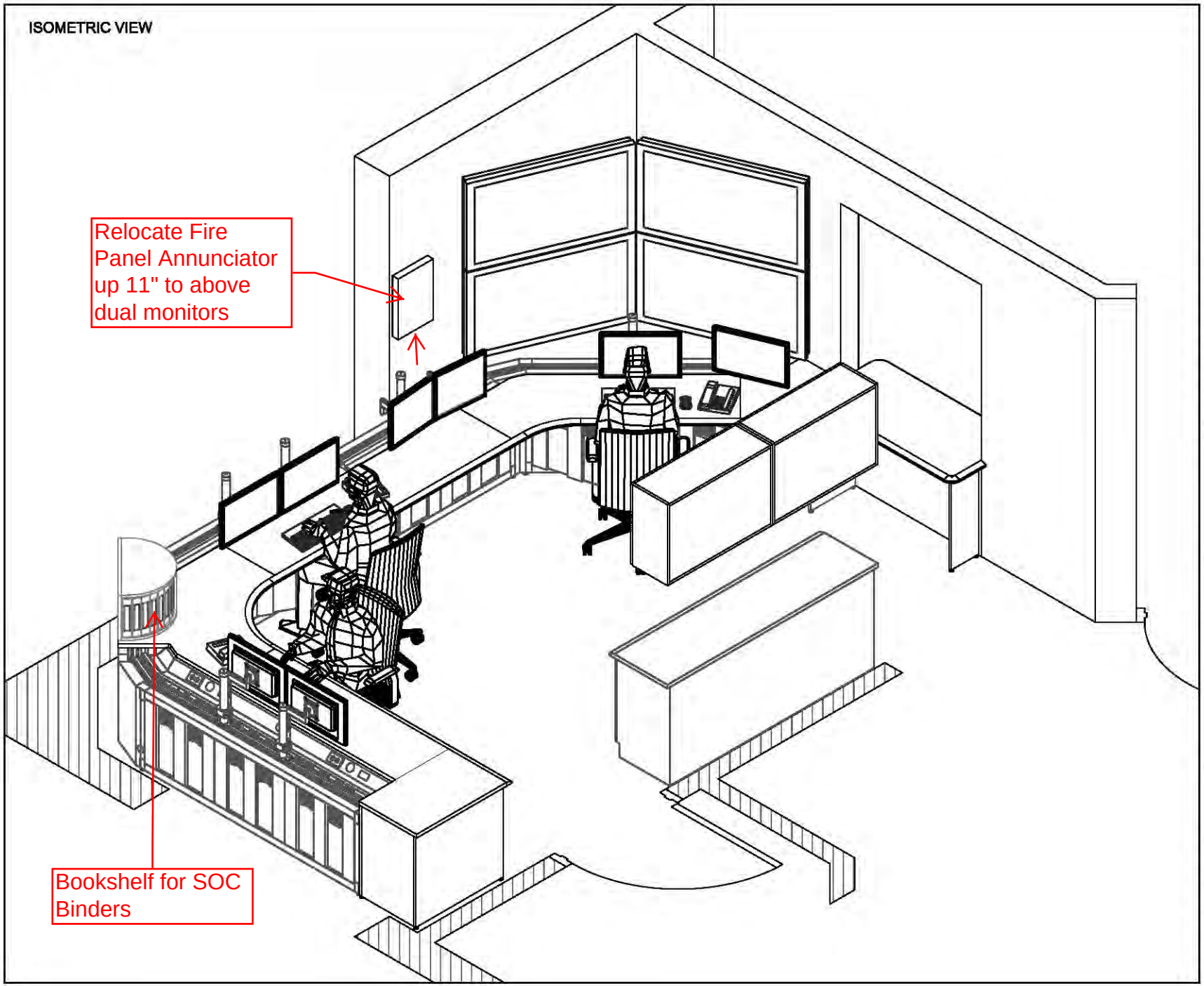
Oregon Convention Center SOC

THIS DRAWING AND DESIGN ARE THE PROPERTY OF THE WINSTED CORPORATION AND MUST NOT BE USED OR REPRODUCED WITHOUT THE WRITTEN PERMISSION FROM THE WINSTED CORPORATION.

Winsted
10901 Hampshire Ave So.
Minneapolis, MN 55438
Phone: 952-944-9050
Fax: 952-944-1546
email: info@winsted.com

Drawing #	DK490
Date	02.18.14
Drawn by	KM
Scale	N.T.S.

ISOMETRIC VIEW



General Notes

CONCEPTUAL

THE INFORMATION HEREIN REPRESENTS A CONCEPTUAL IDEA. MONITORS SHOWN MAY NOT BE TO SCALE.

No.	Revision/Issue	Date

Project

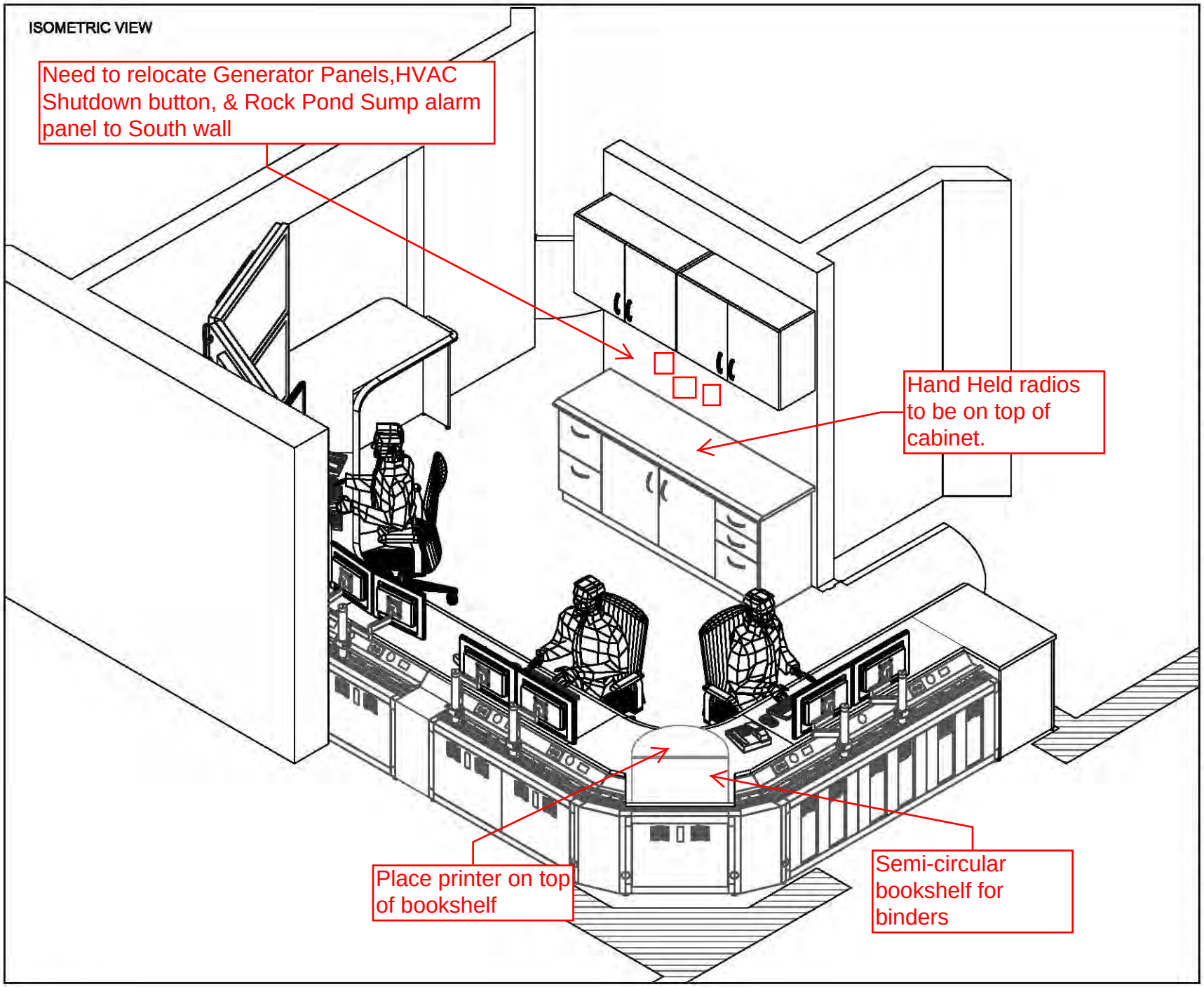
Oregon Convention Center
SOC

THIS DRAWING AND DESIGN ARE THE PROPERTY OF THE WINSTED CORPORATION AND MUST NOT BE USED OR REPRODUCED WITHOUT THE WRITTEN PERMISSION FROM THE WINSTED CORPORATION.

Winsted
10901 Hampshire Ave So.
Minneapolis, MN 55438
Phone: 952-944-9050
Fax: 952-944-1546
email: info@winsted.com

Drawing #	DK490
Date	02.18.14
Drawn by	KM
Scale	N.T.S.

ISOMETRIC VIEW



General Notes

CONCEPTUAL

THE INFORMATION HEREIN REPRESENTS A CONCEPTUAL IDEA. MONITORS SHOWN MAY NOT BE TO SCALE.

No.	Revision/Issue	Date

Project

Oregon Convention Center
SOC

THIS DRAWING AND DESIGN ARE THE PROPERTY OF THE WINSTED CORPORATION AND MUST NOT BE USED OR REPRODUCED WITHOUT THE WRITTEN PERMISSION FROM THE WINSTED CORPORATION.

Winsted
10901 Hampshire Ave So.
Minneapolis, MN 55438
Phone: 952-944-9050
Fax: 952-944-1546
email: info@winsted.com

Drawing #	DK490
Date	02.18.14
Drawn by	KM
Scale	N.T.S.

OCC's Replacement Access Control System (ACS) Specification

The Specification for a replacement ACS for OCC's existing Diamond II ACS will be as follows:

1. The ACS system shall be a web-based system utilizing server appliances and Mercury controllers. The ACS must have an established API with the VMS that allows alarm related OnSSI video segments to be viewed from the ACS web client alarm record screen. The ACS system shall be an S2 NETBOX Extreme Controller System or approved equal.
2. Card Readers will be HID iClass SE, no substitutions
3. Card credentials will be HID iClass SE printable ISO cards, no substitutions
4. All ACS reader controllers will have a power supplies with a minimum of 1 hr of backup battery protection. Power supplies will be Altronix or approved equal.
5. All ACS reader controllers will have circuit surge protection.
6. The ACS Badge Station Printer shall be a dual sided ID ISO-30 badge printer. The ID Badge printer shall be a Magicard Rio Pro or approved equal.
7. The ACS Badge Station ID Photo Camera shall be an 8 MP camera or better with Twain Driver TransTech Trans Cam Solo, or approved equal.

General Requirements--ACS System specifications

1. The security management system shall be implemented through network appliance architecture with a three-tiered modular hardware hierarchy and embedded three-tier software architecture.
2. 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.
3. 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.
4. Security of the data communicated over the network to and from the browser, network controller, and nodes is protected by encryption (SSL 128-bit) and authentication (SHA-1).
5. The top hardware tier is the network controller. Embedded on the Network Controller are an operating system, a web server, security application software, and the database of personnel and system activity.
6. The middle hardware tier is 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 makes 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 are automatically re-integrated.
7. The bottom hardware tier is 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.
8. Temperature Blade: shall support eight analog temperature sensor inputs.

9. The security management system 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.
10. 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 high reliability relational database that is embedded without requiring the use of a separate PC server.
11. 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.
12. The web browser shall provide UL 1076 compliant browser-based monitoring and incorporate asynchronous Javascript™ and XML technology (AJAX) for a faster user experience.
13. The security application software tier contains the business logic. This application shall also be embedded on the network device and requires no additional memory or processing power.
14. This three tiered embedded software design runs within an embedded Linux operating system and shall require no client-side software other than a web browser.
15. All equipment and materials used shall be standard components, regularly manufactured, and regularly utilized in the manufacturer's system.
16. All security management systems and components shall have been thoroughly tested and proven in actual use.
17. All security management systems and components shall be provided with an explicit manufacturer warranty of one year for software and two years for hardware.

Overall System Capability

1 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, 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.

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

3 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.
   a) The widgets that shall be available for a layout are: Activity Log, Clock, Duty Log Entry, Explorer, Events, Floorplans, Intrusion Panel, Passback Grace, PhotoID History, Portal Status, Portal Unlock, Statistics Block, Status, Threat Level, and Video.

4 System Partitioning: The system administrator shall have the ability to divide the S2 system into partitions, allowing subsets of the overall population and/or resources to be managed separately.

a) From the default Master partition, one or more additional partitions can be created.
b) Each partition shall contain some number of administrators, card holders with their credentials, and resources.
c) 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.

5 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.

a) The security management system shall provide the following Access Control capabilities:
   i) Integrated photo ID creation capability with video verification.
   ii) User interface secured access under encrypted password control.
   iii) System-wide timed anti-passback function.
   iv) Regional anti-passback with mustering and roll call functions.
   v) Region occupancy counting and control.
   vi) “First-in-unlock” rule enforcement.
   vii) Multiple access levels and cards per person.
   viii) 128-bit card support for Wiegand card readers.
   ix) Detailed time specifications.
   x) Simultaneous support for multiple card data formats.
   xi) Elevator control.
   xii) Access privileges variable by threat level.
   xiii) Scheduled portal unlock by time and threat level.
   xiv) Card format decoder quickly discovers unknown card formats.
   xv) Card enrollment by reader or keyboard.
   xvi) Compatibility with various input devices, including biometric readers.
   xvii) Activation/expiration date/time by person with one minute resolution.
   xviii) Access level disable for immediate lockdown.
   xix) Use of Threat Levels to alter security system behavior globally.
   xx) Multiple holiday schedules.
   xxi) Timed unlock schedules.
   xxii) Scheduled actions for arming inputs, activating outputs, and locking and unlocking portals.
   xxiii) Card enrollment reader support.
   xxiv) Dual-reader portal support.
   xxv) Wiegand Reader support.
   xxvi) Magnetic-stripe reader support with cards using ABA Track 2 format for up to 200 bits.
   xxvii) Wiegand keypad PIN support for 4-digit or 6-digit PINs.
   xxviii) 8-bit and 4-bit burst keypad support for 4-digit or 6-digit PINs.
   xxix) Integration with supported alarm panels.
   xxx) Optional storage and recall of ID photos and personal/emergency data.
   xxxi) Up to 60,000 person records.

b) The security management system shall provide the following Monitoring capabilities:
   i) Common alarm panel integration for disarm on access, and arm on egress.
   ii) Integrated alarm monitoring and event management with alarm panels.

iii) Support for the direct viewing of IP cameras.

iv) Integrated real-time IP, DVR, and NVR systems with stored video replay for events.

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

vi) Virtual inputs for video loss and building-occupancy-limits-exceeded.

vii) Provides alarms on communication loss and temperature variation.

viii) Support for the creation of custom sets of alarm event actions.

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

x) Available video control and playback through the user interface.

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

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

xiii) Support for electronic supervision of alarm inputs.

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

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

xvi) Support for the creation of unlimited customized monitoring layouts through the use of widgets.

xvii) Graphic floorplans with active icons of security system resources.

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

xix) Secure access to the user interface under encrypted password control

xx) Delivery of alerts via browsers, email, and text messages.

c) The security management system shall provide the following Video Management capabilities:

i) Real-time video monitoring displays, including unlimited cameras simultaneously.
ii) Playback of event-related video.
iii) Video switching and video widget pop-ups based on access activity or event activation.
iv) Integrated alarm inputs from the video management system.
v) Digital playback of video events.
vi) Linking of video and events based on triggers provided by the security management system or video system.
vii) Support for multiple DVR and NVR systems.
viii) Multiple pre-programmed supported cameras.
ix) Recall of photo ID and real-time image for comparison.
x) Monitoring and control through a web browser interface.
xi) System user permissions to grant whole or partial access to system cameras and video resources.

d) The security management system shall provide the following Security Database capabilities:

i) 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.

ii) Partitions: It shall be possible to partition the system to create independent, virtual security management systems for multiple populations.

iii) Support for the sharing of access levels and user privileges across partitions in a system.

iv) Built-in Open Database Connectivity (ODBC) compliant database for personal data.

v) LDAP integration for single-user logon authentication.

vi) Up to 60,000 person records.

vii) Network-secure API for external application integration.

viii) Extensive and easy to use custom report generator.

ix) User-defined data fields in personnel records.

x) Record recall by vehicle tag, name, or card.

xi) ODBC compliant Database.

xii) An API for adding to, deleting from, and modifying the database.

xiii) Storage of system user passwords and permissions.

xiv) Storage and recall of ID photos and emergency personal information.

xv) Pre-defined reports on system configuration, system activity history, and people.

xvi) English-based query language for instant custom reports.

xvii) 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.

xviii) Periodic backup to on-board flash ROM and optional network attached storage (NAS), including FTP servers.

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

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

Hardware Requirements

a) The security management system shall employ a modular hardware concept that enables simple system expansion and utilizes a three-tiered hardware hierarchy:

   i) 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 security management system, set configurations, monitor activities, run reports, and manage alarms.

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

   iii) 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.

   iv) 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. A MicroNode shall also be available that combines an Access Control blade and 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 three configurations to support small to medium, large, and ultra-large systems. Those systems shall be identified respectively as: a solid-state network controller, an enterprise network controller.

c) A solid-state network controller shall consist of a blade-style, circuit card that also combines a network node on the card. The network controller portion of the card shall contain a processor, flash memory, and a network switch. The network controller shall be supplied with 12V DC at a minimum of 3 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 Node portion shall contain a serial port for communication with the Application blades and a network interface port.

d) The local 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.

e) The enterprise network controller shall consist of a 1U rack-mounted controller with additional processing power and memory, disk drive, serial port and network connections. The enterprise ultra network controller shall consist of a 2U rack-mounted controller with additional processing power and memory, RAID-1 disk drive array, serial port and network connections. The enterprise and enterprise ultra network controllers shall have the following capabilities:

   i) Nodes/MicroNodes: 64 (256 for enterprise ultra)

ii) Access control readers: 896 (3584 for enterprise ultra)

iii) Access cards: unlimited

iv) Access levels: 512 per partition

v) Concurrent system users: 35

vi) Alarm input points: 2000 (4000 for enterprise ultra)

vii) Control point outputs: 2000 (4000 for enterprise ultra)

viii) Temperature monitor points: 500

ix) IP, DVR, and NVR cameras: Limited only by license

x) Online event history log: up to 400,000,000 records

xi) Ethernet switch ports: 2

xii) Time specifications: 512 per partition

xiii) Time spec groups: 64 per partition

xiv) Time specs: 8 per group

xv) Threat Levels: 8 per partition

xvi) Threat Level Groups: 32 per partition

xvii) Holidays: 30 per partition

xviii) Access Levels per person: 16

xix) Credentials per person: 100

xx) Report Groups: 50

xxi) Camera Groups: 50

f) 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 12V DC at a minimum of 3 amps. The Node blade shall supply all Application blades in the node with power. The Network Node shall be available in three configurations: a combined network controller/network node blade; a standalone Network Node blade, and a MicroNode with included Access Control blade. Each Network Node shall support up to seven Application blades except for the MicroNodes. Communications between the node and network controller shall be encrypted and authenticated (SHA-1). The Application blades shall interface with the network controller through the Network Node. The Application blades shall be blade-style circuit cards.

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.

Hardware Packaging 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.

Software Requirements

a) Operating System and Application Software:

   i) The embedded operating system for the solid-state network controller shall be Linux® **or approved equal**. The disk-based enterprise network controllers shall use Ubuntu 10.04 LTS (long term support) as the operating platform **or approved equal**. The operating system kernel shall be open-source and no operating system training or certification shall be necessary.

   ii) The security management system application software shall be embedded in the system. The database shall be an embedded PostgreSQL **or approved equal** relational database requiring a small footprint and provides high reliability. The web server shall be based on an embedded Apache™ web server **or approved equal** enabling users to access and operate the system using a standard web browser.

b) Software Licensing:

   i) Software licensing shall be based upon the number of readers and cameras for one network controller board. Software license upgrades shall be available if system reader and camera capaOCC/METRO 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.

   ii) 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: 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 security management system shall be provided with complete embedded documentation. The on-line documentation shall include:

   i) 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.

ii) 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.

iii) 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.

iv) 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.

v) System Administration 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 security management system 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 the secure network.

f) Language Support: The security management system 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.

g) Date Formats: The security management system shall support global date formats as follows:

i) mm/dd/yyyy

ii) dd/mm/yyyy

iii) yyyy/mm/dd

h) Floorplans: The security management system 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.

i) 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.

j) 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 security management system shall maintain person data relating to access control, system user privileges, photo identification, system activity, and contact information.

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

iii) A system user holding at least an ‘Administer’ user role shall be able to create, delete, and modify person records, including access levels.

k) 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 security management system database. Data that shall be importable shall include:

i) LASTNAME

ii) FIRSTNAME

iii) MIDDLENAME

iv) ACTDATE (activation date)

v) EXPDATE (expiration date)

vi) NOTES

vii) TEXT1...TEXT20 (user defined fields 1 through 20)

viii) ACCESSLEVEL1...ACCESSLEVEL32

ix) PERSONID

x) PIN

xi) ENCODEDNUM1...ENCODEDNUM10

xii) HOTSTAMPNUM1...HOTSTAMPNUM10

xiii) CARDFORMAT1...CARDFORMAT10

xiv) BADGELAYOUT

xv) JPEG ID PHOTO

xvi) CONTACT PHONE

xvii) CONTACT EMAIL

xviii) CONTACT SMS EMAIL

xix) CONTACT LOCATION

xx) OTHER CONTACT NAME

xxi) OTHER CONTACT TELEPHONE

xxii) OTHER CONTACT TELEPHONE2

xxiii) VEHICLE 1 COLOR

xxiv) VEHICLE 1 MAKE

xxv) VEHICLE 1 MODEL

xxvi) VEHICLE 1 STATE

xxvii) VEHICLE 1 LICENSE#

xxviii) VEHICLE 1 TAG#

xxix) VEHICLE 2 COLOR

xxx) VEHICLE 2 MAKE

xxxi) VEHICLE 2 MODEL

xxxii) VEHICLE 2 STATE

xxxiii) VEHICLE 2 LICENSE#

xxxiv) VEHICLE 2 TAG#

l) Data Security:

i) 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.

ii) Communication between the network controller and the Network Nodes shall be encrypted and authentication/tamper detection shall be done using the SHA-1 algorithm.

iii) 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.

m) Data Backups: It shall be possible to configure regular automatic database backups.

i) It shall be possible to back up a solid-state network controller to an on-board compact flash.

ii) It shall be possible to back up an enterprise network controller to a built-in hard drive.

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

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

n) On-board Data Management: Each night the security management system 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.

o) Partitions: It shall be possible to create multiple partitions for the management of multiple security systems or multiple populations.

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

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

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

iv) Each partition shall require at least one Node.

p) User Roles and Permissions: There shall be 4 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:

   i) 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.

   ii) Master Partition Administer: 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.

   iii) 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.

   iv) Full System Setup: These users may use the functions of all menus in all partitions.

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

q) Alarm Panels: The security management system shall be capable of integrating with alarm panels, arming the panels, disarming the panels, and triggering events based upon alarm panel status.

r) DMP Intrusion Panels: The S2 system shall be capable of integrating with Digital Monitoring Products (DMP) XR500 Command Processor Panels.

   i) Security administrators can use events on a DMP panel, such as a zone going into an alarm state, to trigger events in the S2 system. They can also use events in the S2 system to control operations on the DMP panel, such as the arming or disarming of an area.

   ii) 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.

s) Alarm Events: The security management system shall be capable of managing alarm events.

   iii) 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 .5 seconds or 1-120 seconds.

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

(1) Lock and Unlock portals.

(2) Activate and Deactivate relay outputs.

(3) Arm and Disarm input groups.

(4) Pulse outputs or output groups.

(5) Arm and Disarm alarm panels.

(6) Send emails and SMS messages.

(7) Move cameras to preset positions.

(8) Switch to a video monitor.

(9) Record video.

(10) Momentarily unlock portals.

(11) Display ID photos.

(12) Change the system threat level.

(13) Make entries in the activity log.

(14) Play a digital sound file.

(15) Display alarms in different colors.

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

(17) Require a duty log entry.

(18) Clear alarm automatically or require an acknowledgement.

v) 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.

vi) It shall be possible to trigger events based on system activity such as:

(1) Video motion detection.

(2) Camera failure and camera restore events.

(3) Valid or Invalid card reads.

(4) Portals held or forced open.

(5) Valid card reads with a specified access level.

(6) Inputs entering an alarm state.

(7) High and low temperature events.

(8) Alarm panel arming failures.

(9) Alarm panel zone faults.

(10) Tailgating and passback violations.

(11) Occupancy limit violations.

(12) Zone empty violations.

(13) Node power failure, communication failure, timeout, and tamper events.

t) Activity Monitoring

i) The security management system shall support a Monitoring Desktop that integrates video, system activity logs, floorplans, ID photos, and alarm notifications. Activity Log viewing includes one-click navigation to person records.

ii) 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.

iii) 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.

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

u) Network-based Camera and Video Surveillance: The system shall provide live IP video surveillance capability. The number of supported cameras shall be limited only by license. The system's video capabilities shall include video monitor switching based on access activity. The system shall provide monitoring, configuration, and administration of IP video. Cameras can be separately monitored or monitored in groups.

i) Presets: The system shall support the creation, deletion, and editing of camera preset positions in the system. It shall also be possible to save changes in preset positions directly to a camera website.

ii) Views: The system shall support the creation, deletion, and editing of multiple camera views, specifically Quad views (four cameras). The application shall provide a drop down pick list for selecting current views or naming of new views.

v) Access Control:

i) The security management system 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.

ii) 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.

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

(2) Time specifications shall function appropriately per node for the time zone specified for that node

iii) Card Formats: The system shall support the use of readers that use the Wiegand Reader Interface. The system shall default to the Wiegand 26 bit format unless a different bit length format is created in the system. 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.

(1) 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.

(2) 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.

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

iv) Access Levels: The system shall be capable of storing up to 512 access levels in each partition. Each access level must be assigned a unique alphanumeric name of up to 64 characters. The definition of an access level shall require the assignment of a reader or reader group, and a time specification. It shall be possible to also assign an elevator floor group to an access level.

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

vi) 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.

vii) Portals: A portal is any access point and each portal supports up to two access reader devices. 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:

(1) Card readers and keypads.

(2) Output for locking.

(3) Input for monitoring the door switch.

(4) Input for a Request-to-Exit function.

(5) Local alarm outputs and system alarm events.

viii) 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.

(1) 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.

ix) Portal Alarm Conditions: Portals shall have four alarm conditions. The four alarm conditions are as follows:

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

(2) Held: When a portal is held open past the expiration of the shunt timer.

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

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

x) 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.

xi) 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.

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

(2) It shall also be possible to set a specific time for all cardholders to be Graced daily.

(3) The system shall be able to automatically place the cardholder in a predefined region upon the selection of the grace option

xii) 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.

xiii) Scheduled Actions: It shall be possible to specify system actions to occur at scheduled times. These actions can include:

(1) Arming and disarming inputs.
(2) Activating and deactivating outputs.
(3) Locking and unlocking portals.

xiv) Floorplans: 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.

(1) 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.

xv) 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.

(1) 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.

xvi) A security management system user holding a "Setup" user role shall be able to create, delete, and edit access control specifications.

w) Threat Levels:

i) 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.

ii) The security management system shall support 32 threat level groups.

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

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

x) Reports:

i) The security management 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. 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.

ii) It shall also be possible to produce reports directly from the network controller based on data in archive files on FTP servers, network attached storage, or the controller-attached compact flash.

iii) The security management 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.

iv) 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.

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

vi) The specific reports provided shall include the following:

(1) Configuration Reports

(a) 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.

(b) Cameras: Displays all camera configuration information including control address, IP port, and camera type.

(c) Camera Presets: Displays configured presets for each camera in the system.

(d) Elevators: Displays elevator configuration information including Node, Reader, and Floor to output mappings.

(e) Floor Groups: Displays all configured floor groups for use in elevator control.

(f) Holidays: Displays holiday specification information.

(g) Portals: Displays portal definition information including reader, DSM input, REX input, alarm outputs, and events.

(h) Portal Groups: Displays a list of all defined portal groups.

(i) Reader Groups: Displays defined groups of readers.

(j) Resources: Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.

(k) Threat Level Groups: Displays all configured threat level groups and the threat levels assigned to them.

(l) Threat Levels: Displays all configured threat levels including the description and color assignment.

(2) History Reports

(a) 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.

(b) 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. Report results can be printed, output to a PDF file or put into a spreadsheet.

(c) 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.

(d) Portal Access Count: Display how many times users have used a portal.

(e) 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.

(3) People Reports

(a) Access Levels: Displays all access levels entered into the system including time specification, reader/reader group, and floor group.

(b) Current Users: Displays a list of all security system users currently logged in to the security system website.

(c) 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. Report results can be printed, output to a PDF file or put into a spreadsheet

(d) 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.

(e) Photo ID Gallery: Displays all the photo ID pictures in the system and the person's name.

(f) Photo ID Requests: Displays all outstanding badge print requests and lists ID, name, badge layout, activation date, request date.

(g) Portal Access: Lists people with access for a selected portal.

(h) Roll Call: Allows you to select a defined Region from the drop-down and see a list of people currently in that region.

(i) Roster: Displays every person entered into the system and it lists name, ID photo, expiration date, username, and access level.

(j) Time Specifications: Displays all defined time specifications currently in the system.

y) Administration: The security management system 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 security management system 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) 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 compact flash onboard the solid-state network controller, and written to the drive on the disk-based controller.

(b) Backups shall also be written to network attached storage (NAS) or an FTP 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 board storage by the system user at any time.

(2) 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.

(3) 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 .tgz 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.

(4) File cleanup: A utility shall be provided to assist in file cleanup. This utility will display for review and deletion all floorplan jpeg files, photo IDs, database backups, badge layouts, and software updates.

(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 system 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 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.

(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. Passwords may contain neither double-quote (“) nor single-quote (‘) characters.

(b) It shall also be possible to integrate an LDAP 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 a drop-down list.

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

(9) Enrolling new people: 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 Administer user role. Person data can be added, deleted, and edited by such system users.

(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 photo ID functions entirely from within the browser

(11) 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.

(12) Configuring network resources:

(a) LDAP: It shall be possible to configure an LDAP server for directory services and single-user login. This will reference the LDAP-stored password for use by the system.

(b) DNS: The system shall support setting IP addresses for up to two domain name servers.

(c) 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.

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

(e) 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.

(f) 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.

(g) A system user holding 'Setup' permissions shall be able to configure network resources.

Video Management Integration

i) General: The security management system shall support the integration of Digital Video Recorders (DVR) supporting analog video cameras and 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.

ii) Integrated DVR/NVR Systems:

(1) Dedicated Micros – DVR DS2 or DV-IP

(2) exacq – exacqVision

(3) JVC – VR900

(4) Milestone Systems – XProtect Enterprise, XProtect Professional, XProtect Corporate

(5) OnSSI – NetDVMS, NetDVR

(6) Panasonic Digital Disk Recorder – WJ-HD309a, WJ-HD316a

(7) Salient Systems CompleteView NVR

(8) Vicon – ViconNet

ii) OVID: Open Video Interface API:

(1) This specification defines an API to implement the integration of video surveillance systems with the security management system.

(2) The OVID API shall allow users to monitor and control one or more video servers along with their associated video cameras, to augment the physical security devices (door locks, card readers, etc.) controlled by the security management system.

(3) The integrated system shall be controlled through a web browser user interface which presents an integrated view of both the security management system and the video surveillance system.

iii) LDAP: It shall be possible to configure and Active Directory Server with the security management system.

(1) This shall provide single user-login capability.

(2) Password rules and authentication will be governed by the LDAP server.

Mercury Hardware Integration

i) The system shall support the integration of access control hardware from Mercury Security Corp.

ii) The following Mercury hardware components shall work with the controller:

(1) Supported Mercury Panels:

(a) EP2500: Intelligent Controller: 32 MB RAM, Ethernet

(b) EP1502: Intelligent Dual Reader Controller: 16 MB RAM, Ethernet, 2 readers (magnetic stripe or Wiegand) 8 inputs, 4 relays

(c) EP1501: Intelligent Single Door Controller: PoE, single door, 2 readers, 2 inputs, 2 outputs

(2) Supported Mercury Interface Boards (SIOs)::

(a) MR-50 Reader Interface Module: 1 reader (magnetic stripe or Wiegand), 2 inputs, 2 relays

(b) MR-52 Reader Interface Module: 2 readers (magnetic stripe or Wiegand), 8 inputs, 6 relays

(c) MR-16in Input Monitor Module: 16 inputs (zones), 2 relays

(d) MR-16out: Relay Output Control Module: 16 relays

Otis Elevator Compass™ System Integration

i) The system shall support the integration of the Otis Elevator Compass™ Destination Entry System with the security management system. The Compass system is designed to optimize the use of elevators in large office buildings.

(1) The boundary between the Compass network and the security management system network is a Layer 3 switch. This switch routes two-way data traffic between the controller and the Compass nodes, using the TCP/IP networking protocol.

(2) The controller acts as the central processor for the security system. A single controller can supervise the operation of many nodes. It also manages all communication between the security management system and the Compass system.

(3) The Network Node is a peripheral processor which handles building security hardware such as card readers. A node can control many readers.

(4) Once the system has been initialized to support an interface to the Compass system, standard security management system configuration pages can be used to configure the Compass system:

(a) The Status page lets users view the Compass IP network configuration information, such as node status.

(b) The Floor Map page lets users configure the floor mapping needed to identify the building floors by name and floor.

(c) The Configuration page lets users configure the destination entry server (DES) nodes, destination entry director (DER) nodes, and destination entry computer (DEC) nodes in the Compass system.

(d) The Events page lets users view the IP address, name, node type, and status of each node in the Compass system.

(e) The Reader Groups and Access Levels pages let users configure reader groups and their associated access levels within the Compass system.

Remote Lockset Integration

The system shall support the integration of ASSA ABLOY Wi-Fi enabled locksets (models vS2 and pS2) with the security management system.

i) 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.

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

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

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

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

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

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

viii) 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.

API Integration

An Application Programming Interface (API) is provided for the security management system. The API provides programmatic access to the network-connected components managed by the security management system.

i) Communication between the security management system and another application takes place through the TCP/IP networking protocol. The API is invoked by POSTing an HTTP message to the web server on the network controller.

ii) The security management system database includes a table of “people” whose records act as container objects for attributes attached to people in real life. People are mapped to access levels, which specify access privileges—and to access cards, whose credentials are used for access control.

iii) Access levels are entered into the system using the normal web user interface for the security management system. People and credentials may be entered into the system either through the web user interface or through the API.

iv) The API supports commands for:

   a) Adding, modifying, removing, and retrieving data about a person, and retrieving information about one or more people based on various search criteria.

   b) Adding, modifying, and removing credentials, and retrieving a list of the names of defined card formats.

   c) Adding, modifying, and deleting access levels, and retrieving a list of the valid access levels in the system.

   d) Pinging the security management system to determine its health, and retrieving the current version of the API from the server.

   e) Retrieving a history of access activity, either for all users or for a particular access card.

   f) Adding, modifying, and removing threat levels and threat level groups, and setting the threat level in the system.

g) Retrieving a list of portals and associated card readers defined for the security management system.

h) Adding, modifying, deleting, and retrieving time specifications and time specification groups.

i) Adding, modifying, and deleting holidays, and returning a list of holiday keys or a specific holiday.

j) Adding, modifying, deleting readers and reader groups, and returning a list of reader group keys or information for a specific reader group.

k) Adding, modifying, and deleting portals and portal groups, and retrieving information about a specific portal group.

l) Requesting events from the Activity Log that occurred within a specified time period. These events are returned from the API in the CSV Export report format.

Certifications

i) UL 294 listed or as listed by a national recognized testing agency to meet the requirements of State of Oregon Electrical Code.

ii) ISO 9000 listed.

Card Reader and Credential Specifications

i) HID iClass card readers will be utilized for this installation.
ii) Qty of 1000 HID 200x iClass Credential card stock will be required for this installation.

Pricing Schedule

State Initial Warranty Period of Proposed Equipment & Software:

VMS: One Year

ACS: One Year

System Pricing	
	Pricing
SOC Console Pricing	$ 67,738.00
VMS System Pricing	$152,484.00
ACS System Pricing (Addressed in Alternate 18)	$ 77,490.00

Alternates Camera Options	
CAMERAS	***Pricing***
Alternate 1 – New Camera 2 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,772.00
Alternate 2 - New Camera 3 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,953.00
Alternate 3 – New Camera 4 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,933.00
Alternate 4 – New Camera 5 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,933.00
Alternate 5 - New Camera 7 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,752.00
Alternate 6 – New Camera 8 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 3,060.00
Alternate 8 - New Camera 10 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,999.00

Alternates Camera Options - Continued	
Alternate 9 – New Camera 11 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 3,008.00
Alternate 11 – New Camera 13 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,786.00
Alternate 12 – New Camera 14 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,933.00
Alternate 13 – New Camera 15 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,933.00
Alternate 14 – New Camera 19 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,792.00
Alternate 15 – New Camera 23 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 2,417.00
Alternate 16 – New Camera 25 with LS Channel License & "Current" prorated to 2/7/2015 Total System Installed Price	$ 3,008.00

Alternate Card Reader Options	
	Pricing
Alternate 18 – Provide S2-EXT-32-RM Netbox Extreme Controller with OnSSI Occularis "LS" API and other ACS equipment required to replace existing Diamond II ACS. Total System Installed Price including 1-yr SUP	$ 77,490.00
Total System Installed Price	**$337,997.00**

Line Item Equipment Pricing of Components	
Item	***Pricing***
ACS Intelligent Reader Mercury Controller S2-EP-2500	$1,460.00
ACS 16 Input Module S2-MR-16 IN	$ 567.00
ACS 16 Output Module S2-MR-16 OUT	$ 567.00
MR50 Reader Interface Module/1 Reader S2-MR-50	$ 260.00
8-Port Multi Device Interface Panel S2-MUX-8	$ 470.00
HID iClass SE RP10 Mullion Reader	$ 124.00
HID iClass SE RP40 Wall Switch Reader	$ 202.00
HID iClass SE RPK 40 Wall Switch with Key Pad Reader	$ 325.00
1000 HID iCLASS SE photo printable ID badge card stock/ Model 300	$2,910.00
1.3 MP Sony SNC DH160 Interior Mini Dome IP Camera	$ 781.00
3.0 MP Sony SNC DH260 Dome IP Camera w/IR	$ 951.00
3.0 MP Sony SNC DH240T Dome IP Camera Wide Dynamic	$1,602.00
1.0 MP AXIS P3354 Indoor Dome camera	$ 560.00
1.0 MP AXIS M3006-V Wide Angle Lens	$ 466.00
1.0 MP Sony SNC-EP 550 340° PTZ w/28x, UNI WMB3 & UNI-INL7C2 enclosure.	$2,177.00
OnSSI Occularis LS base Server License	$2,403.00
OnSSI Occularis LS Camera Channel License	$ 283.00
OnSSI Occularis Camera Channel License software upgrade plan “CURRENT” —1yr	$ 57.00
OnSSI Occularis Camera Channel License software upgrade plan “CURRENT”—3yr	$ 121.00
ACS Software Upgrade Plan for 1-year	$ 600.00
ACS Software Upgrade Plan for 3-years	$1,530.00

2.6 Contractor's Labor Rates	
Positions	***Rate/Hr***
Project Manager	$ 96.00
CAD Drafting Technician	$ 85.00
Cable Technician	$ 90.00
Equipment Installation Technician	$ 90.00
Engineering Technician	$ 96.00
Training Technician	$ 90.00
Service Technician	$114.00

CONFIDENTIALITY AGREEMENT

THIS CONFIDENTIALITY AGREEMENT ("Confidentiality Agreement") is made effective as of the last date of signature below (the "Effective Date"), by and between the Metropolitan Exposition Recreation Commission, an appointed commission of Metro, a metropolitan service district established pursuant to Oregon law and the Metro Charter, whose address is 600 NE Grand Avenue, Portland, Oregon, 97232, ("MERC"), and CONVERGINT TECHNOLOGIES, referred to herein as "Contractor" located at 7678 SW MOHAWK ST TUALATIN OR 97062.

BACKGROUND

A. Under Metro Request For Bids No. RFP 2519, MERC is seeking bids from qualified firms to provide security equipment for the Oregon Convention Center ("OCC");

B. MERC wishes to make available certain information regarding the security design at OCC to Contractor, but only with certain safeguards to protect against unnecessary or inadvertent disclosure;

C. The parties enter into this Confidentiality Agreement to protect the confidentiality of certain information as set forth herein and to prevent the unauthorized disclosure of such information as further described below.

AGREEMENT

NOW THEREFORE, the parties agree as follows:

1. From the Effective Date of this Confidentiality Agreement and all times thereafter, Contractor and its employees, agents, independent contractors, officers and directors, and successors and assigns, to the extent not prohibited by law, shall keep in confidence and not disclose the OCC Integrated Security Design ("the Confidential Information") to any person or entity; except that the Contractor may disclose the Confidential Information:

   a. Upon MERC's prior written consent;

   b. In response to a valid order of any court, or a demand or request for information from a government agency made pursuant to the agency's duly vested powers or authority to do so;

   c. In response to a properly served, valid and unchallenged subpoena, notice of deposition, or other discovery request;

   d. Pursuant to any resolution, order, or determination of MERC that such disclosure is in the public interest; and

   e. As otherwise required by law.

2. The parties to this Confidentiality Agreement shall notify one another in writing of any subpoena, notice of deposition, discovery request, demand, or order described in Paragraph 2.b. or c. within seven (7) days of receiving such notice.

3. Contractor shall restrict the transmittal of the knowledge and the substance obtained to its respective officers, directors, agents, independent contractors, employees and attorneys who are directly connected with the Bid and who require such information. Contractor shall take reasonable actions to ensure that all such persons and their employees, agents, independent contractors, officers and directors, and successors and assigns do not disclose any information, using the same level of care to preserve the Confidential Information that Contractor would accord to its own most confidential information. Once Notice of Award of the Bid for this work goes out to all Bidders, Contractor will immediately destroy the Confidential Information if Contractor was not the successful Bidder on the project.

4. Any notice required or permitted under this Confidentiality Agreement shall be (a) in writing, (b) dated as of the date delivered or sent, and (c) delivered in person or by messenger, or sent by facsimile with proof of receipt by addressee or by Federal Express or a similar overnight delivery service, or by United States certified mail, return receipt requested, postage prepaid. The address and facsimile numbers for each party are as follows:

MERC:
MERC
Attn: Nathan A.S. Sykes
Office of Metro Attorney
600 NE Grand Avenue
Portland, Oregon 97232-2736
Telephone: (503) 797-1544
Facsimile: (503) 797-1792

Contractor:
CONVERGINT TECHNOLOGIES
7678 SW MOHAWK ST.
TUALATIN OR 97062

5. Any party may at any time change its address for notice purposes by giving notice in accordance with this paragraph. Notices shall be deemed given and received on the date of delivery, if delivered in person or by messenger; on the date of receipt if sent by facsimile or through an overnight delivery service; or two (2) days (excluding Sundays and legal holidays) after the date of mailing, if mailed.

6. This Confidentiality Agreement shall be binding upon and inure to the benefit of the parties' successors and assigns.

7. This Confidentiality Agreement shall be governed by and construed under the laws of Oregon.

CONTRACTOR

By: _____

Title: GENERAL MANAGER

Date: 7/24/14

METRO

By: _____

Title: Procurement Manager

Date: 7/24/14