Type of Facility Represented	**Access control point and perimeter intrusion detection and surveillance systems for an OCONUS federal facility (United Nations Headquarters Building)**
Firm's Name	**ECSI International, Inc.**
Name of Project	**Design-Build Project Access Control Technology**
Location of Project	**Addis Ababa, Ethiopia**
Owner	**United Nations Economic Commission for Africa**
Summary of Project Role	**ECSI was a subcontractor to a Prime Contractor. ECSI self-performed 100% of its scope – site survey, design and engineering, assembly and integration, factory test, installation supervision, and depot level support.**

Project Description: ECSI executed a task order to renovate/modernize gate automation, perimeter intrusion detection, and surveillance systems at UNECA headquarters in Addis Ababa, Ethiopia. ECSI was a subcontractor in a DB team. ECSI work scope included: site surveys, design and engineering in accordance with UN requirements; preparation of submittals drawings and specifications; selection, acquisition, assembly and integration of systems and components and quality control oversight to meet UN performance specifications for automating gates, enhancement of perimeter security detection and surveillance, and implementation of primary and secondary command and control centers; preparation and execution of factory test and inspection, periodic installation supervision: integration and final testing; preparation and execution of training plans; and provision of post installation depot level support.

Facility Size: UNECA is an enclosed campus consisting of five main buildings set on approximately 25 acres in the heart of Addis Ababa. The campus is enclosed by a combination of fence and a stone wall with a perimeter of approximately 4,500 feet. The existing perimeter included three entrance gates; VIP West Gate and two gates on the East side for vehicles and pedestrians. The project scope included expanding the perimeter security system to include a new area of approximately 6 acres requiring full perimeter security and surveillance for an additional 1,500 feet.

Project Execution

Phase 1 – Site Survey

Using its site survey procedural handbook, ECSI planned and completed an extensive site survey (3 weeks in-country) of all gates, perimeter security systems, CCTV systems, infrastructure and facility systems. At the conclusion of the site survey, ECSI prepared and submitted a Scope Validation Report for review and approval by the client. The report documented existing conditions, identified any discrepancies with the RFP and provided recommendations for improvements, system by system and item by item. ECSI found gaps in the perimeter security that the UN was unaware of and that would have to be addressed to provide the required perimeter protection. ECSI also tested all equipment identified for integration into the new system and found some of the existing equipment had adjusted, repaired or replaced to work effectively

with the new systems upgrade. The survey also indicated there were physical and infrastructure issues, such as the existing conduits on site were not adequate for the new system requirements.

The engineering staff and engineering management were the principal participants in developing the risk management program for this project. Risks were evaluated and mitigation plans were developed. The risks for this program were considered low. The program involved straightforward engineering and was accomplished without any major issues. Management of ECSI under the ISO 9001:2008 certification assures that management maintains controls over operations and that by scheduled audits strives for continual improvements in management and overall operations.

Phase 2 – Design Development

ECSI designers prepared the necessary design and engineering drawings to document the physical, electrical, and network requirements of the project. These drawings included civil drawings showing physical placement of all elements including any foundation or mounting details

The project included three (3) access control points: the VIP gate, the Employee/Visitor gate, and the Cargo gate; and perimeter intrusion upgrade. The VIP gate provides vehicle and pedestrian access to a conference facility that hosts frequent international meetings. The gate included existing K-12 pop-up bollards and swing gates that were manually operated. The ECSI design included a gate automation package consisting of entry and exit lift arm gates that are controlled by smart card (employee) and bar code card (contractor and visitor) readers to control the gates after a valid card read has been processed. An existing pedestrian turnstile was automated similarly with smart card and bar code readers.

The Employee/Visitor gate was a new gate in the expansion area that included a vehicle inspection area, vehicle entry control with one entry lane and one exit lane; and personnel entry control through a visitor center. The vehicle entry control design included a gate automation package consisting of entry and exit lift arm gates that are controlled by smart card (employee) and bar code card (contractor and visitor) readers to control the gates after a valid card read has been processed. All pedestrians gain access to the UNECA campus through the visitor center where two existing waist-height turnstiles was automated similarly with smart card and bar code readers. Visitors are required to present identification, get photographed, and then are issued a bar code card to be used at the turnstile. A total of eight visitor badging work stations (with camera and printer) were provided as part of the design.

The Cargo gate was a new gate and included a gate automation package consisting of entry and exit lift arm gates that are controlled by smart card (employee) and bar code card (contractor and visitor) readers to control the gates after a valid card read has been processed. Two new pedestrian turnstiles were installed and automated similarly with smart card and bar code readers. Since this gate is used primarily by trucks, the design included a high-low arrangement of the smart and bar code readers.

At each of the gates, cameras were positioned to provide situational awareness of gate activity using a combination of fixed and PTZ cameras. Each gate's guard house is equipped with a workstation to monitor and view the gates activities. The workstations are connected to the redundant security system servers in a secure equipment room interior to the campus.

The existing perimeter intrusion detection system consisted of a single technology that was deployed along the perimeter to detect intrusions. There were cameras associated with the 32 detection zones, but there were many false alarms. The ECSI design added seven additional devices to the existing perimeter and 15 devices for the new perimeter. In order to address the false alarm issue, ECSI designed a video based intrusion detection system that used upgraded cameras with video analytic capability to replace the existing

cameras on the existing perimeter and additional new cameras to be used along the new perimeter. This new video based intrusion detection system provides a second line of defense, and by logically combining both systems, reduces the false alarms completely.

ECSI designed and commissioned a campus-wide fiber optic network for data, video, and voice. This network was designed to take advantage of the existing campus network infrastructure by adding capacity to support the additional data handling requirements required by the cameras, additional alarms and intercom traffic. The design incorporated redundancy at the core switch level increasing the survivability of the security system in the event of an outage or attack.

The facility had cameras and alarms, but they were not integrated. Further, the cameras and alarms were separated into two Security Control Centers, neither of which could see the other's cameras or alarms. ECSI designed an integration solution that converted the existing cameras to digital so that the camera video could be distributed over the expanded campus network to both locations as well as to the Chief of Security's office. The design now meant that operational and system redundancy was built into the overall system and all cameras could be monitored at both locations without requiring more than two operators to monitor all alarms, cameras, and card readers at a single location.

The core of the security system included redundant access control servers, digital video encoders, network video recorders and integration with an existing storage area network (SAN) for archival storage of video and data. The system was designed so that in the event of a failure of one of the servers, the system would continue to operate without interruption until the other server was brought back on line and they were synchronized.

ECSI developed detailed acceptance test plans and a training program for the entire system. ECSI prepared operator and administrator instructions, system documentation and modifications required to meet UN requirements prior to installation and onsite checkout.

Energy Efficiency **–** ECSI uses all low-voltage equipment and power consumption is minimized based on energy efficient equipment of the system.

Sustainability **–** ECSI's system is configured to be controlled by one or two people in a central area, maximizing control and maximizing response time. ECSI also specifies sufficient spare parts (5% to 8%) shipped to the site at the same time as the installation. This not only facilitates final system inspection replacements, but also allows operations to replace equipment and systems immediately should they fail at any time.

The ECSI design used any available conduit and power sources, especially UPSs and emergency generators for its scope of work, reducing the need for additional material and equipment. Where possible, ECSI used existing conduits for new wiring.

As a result of the site survey, ECSI was able to refurbish many of the non operational perimeter security devices and cameras.

Innovative Elements **–** There were multiple challenges associated with this project, which ECSI addressed successfully, including:

1. Design and implementation of a campus-wide fiber optic network for data, video and voice.

2. Design and integration of physical gate automation elements to fit within existing available space to minimize demolition and construction requirements.

3. Design and implementation of the perimeter security system to enhance the performance of the existing detection system, while expanding and adding video surveillance and recording capacity.

4. Design and implementation of primary and back up command and control centers.

Phase 3 – Implementation

During fabrication, ECSI worked with the customer and UN representatives from New York and Ethiopia to complete acceptance testing in ECSI's factory in New Jersey. This allowed for all components to be tested before shipment and installation on the site. The process was complicated by having to communicate and send secure systems information through UN's secure network. ECSI's fabrication managers and in-country support people were in communication continually during fabrication of the equipment, coordination of local supplier procurements (conduits, wiring), and coordination of testing in both the factory and on site.

Systems were air freighted to the site through a freight forwarder, through local customs, and received by UN officials. ECSI then inspected all materials in the UN secure warehouse to insure there was no damage. As is ECSI's practice for timely installation and testing, it also shipped approximately 5-8% spare parts. Should a system or equipment fail during testing, it could be replaced quickly. This also would facilitate maintainability for future operations as all materials are on site.

During the installation phase, ECSI personnel were on site to monitor installation (executed by the Prime Contractor), and provided quality control oversight and technical support to its subcontractor. At the same time, ECSI worked closely with UNECA security management to develop a concept of operation that was implemented within the system configuration programming. This included defining alarm messages and cameras to be displayed; converting an existing employee data base to be used in the new access control system. ECSI then completed on-site testing, final commissioning, and training on the system. ECSI provided in-depth training to security, facilities and IT/network personnel in the management, maintenance, and operation of the new system.

The UN facility used an old analog CCTV system and ECSI installed an IP digital video system and worked out a transition plan that would transfer from old to new systems over two weekends. To accomplish this, ECSI designed a video distribution system that paralleled the video to both the old and new system to facilitate the transition. Once the new digital video system was installed and tested, ECSI implemented dual operations in the Security Control Centers so that security operations never lost their ability to monitor the video cameras. Once fully transitioned, the analog cameras were then operating on the new system. At the completion of the project, new IP cameras were added for surveillance and assessment along the perimeter and in critical interior locations.

Phase 4 – Post Completion Support

ECSI complied with UN security requirements using UN servers, as well as communicating via telephone and email where security issues allowed. ECSI also employed two in-country support people who were in communication directly with the prime contractor and facility operations, both during fabrication of the equipment and during testing and commissioning.

Through its Depot support program, US-based ECSI system specialists could communicate with on-site operations personnel to trouble-shoot any problems that might arise. If there was an equipment failure, sufficient replacement parts were available immediately and additional spare parts could be ordered. To date, there have been no system failures.

Project Evaluation

Quality **–** On this project, equipment delivery has been judged to be excellent. ECSI is ISO 9001:2008 compliant and all purchasing, manufacturing, assembly, packaging and shipping are tightly controlled under the ISO system. Factory test and demonstration were provided as a no-cost option to the customer. The test was successfully conducted and the customer was satisfied prior to shipment to site.

Effectiveness of Management/Business Relations **–** ECSI, as the subcontractor, provided an extensive site survey and prepared a report that documented site conditions, systems failures, and made recommendations for repair and upgrades. Design was developed around these approved upgrades and ECSI coordinated with UN (New York and in-country) through a UN-dedicated server to coordinate fabrication and factory acceptance testing. ECSI developed and provided complete training to security operations and IT/network personnel for use, maintenance, and troubleshooting system issues, should they occur. ECSI also specified sufficient spare parts (5% to 8%) shipped to the site at the same time as the installation. This not only facilitates final system inspection replacements, but also allows operations to replace equipment and systems immediately should they fail at any time. ECSI also designed redundant capability on all network, servers, and many work stations.

Timeliness **–** The engineering staff and engineering management were the principal participants in developing the risk management program for this project. Risks were evaluated and mitigation plans were developed. Due to ECSI's detailed site survey and acceptance testing during fabrication in New Jersey, the risks for this program were considered low, the primary risk being timely receipt of material and equipment. ECSI used a freight forwarder and all shipments were received in time and in good condition. Equipment delivery was consistent with ECSI compliance with ISO 9001:2008, including purchasing, manufacturing, assembly, packaging and shipping, tightly controlled under the ISO system. In-country personnel provided quality oversight of installation and completed the integration, testing, commissioning and testing of all systems.

Compliance with Labor Standards **–** ECSI has a local in-country support group that complied to local and UN facility labor standards.

Compliance with Safety Standards **–** As part of the general contractor's team, ECSI complied with all contractor and UN facility safety requirements and participated in daily safety meetings.

Small Business Utilization **–** ECSI, as subcontractor, self-performed 100% of its scope under the Prime Contractor.

Challenges Encountered/Corrective Actions Taken **–**

Challenge: ECSI was required to use the UNs secure network system for systems communications. The existing network did not have the capacity for the bandwidth demands imposed by the video system required to meet the SOW.

Solution: Working with the UNECA IT department, ECSI devised a design approach that upgraded the core switches on the network for the expanded bandwidth requirements so that the existing network speed could be upgraded to gigabit rates using the existing cable plant. Once that was agreed to, ECSI designed a fiber optic system to accommodate the video signals from the existing and new cameras.

Challenge: The site survey uncovered gaps in the intrusion detection coverage on the perimeter that needed to be closed in order that there be a complete solution provided at the end of the project.

Solution: Working with the security department after the scope validation, ECSI was able to devise a design that would reposition certain devices to cover some of the gaps, thereby requiring fewer new devices to complete the coverage of the perimeter.

Challenge: There were physical connectivity issues and the available conduits were not adequate. Specifically, to be able to combine the video from the two security control centers, cables were required to

be pulled between buildings where there was no feasible way to accomplish it without a costly and time-consuming effort.

Solution: ECSI's analysis showed that while there was not enough conduit capacity available to pull the required cable, there was room for a smaller cable. ECSI devised a design that used a converter that took in the individual device inputs and outputted them onto a single cable. At the other end, a similar device was used to reverse the process.