

**City and County of Honolulu**  
**Department of Transportation Services**  
**Rapid Transit Division (RTD)**

**CORE SYSTEMS**  
**DESIGN-BUILD-OPERATE-MAINTAIN**  
**CONTRACT**

TECHNICAL PROVISIONS  
TP-7 DIVISION 28  
ELECTRONIC SAFETY AND SECURITY  
**ISSUE FOR PROPOSALS – NOT FOR CONSTRUCTION**

**August 17, 2009**

Prepared for:  
**Honolulu High-Capacity Transit Corridor Project**

Prepared by:  
***Parsons Brinckerhoff***  
General Engineering Consultants (GEC)



## **TABLE OF CONTENTS**

### **DIVISION 28 – ELECTRONIC SAFETY AND SECURITY**

28 16 00 Intrusion Detection System



**SECTION 28 16 00**  
**INTRUSION DETECTION**

**PART 1 – GENERAL**

**1.01 SUMMARY**

- A. Description: The Work specified in this section consists of designing, furnishing, installing, and testing the Intrusion Detection System (IDS) to form a complete coordinated system ready for operation throughout the Honolulu High-Capacity Transit Corridor Project (HHCTCP).
1. Provide IDS at all locations and devices where general public access is prohibited or where public access requires emergency response, including, but not limited to, the following:
    - a. All gates at TPSS and GBS sites
    - b. Non-public spaces and rooms at stations and rooms in MSF buildings
    - c. End-of-platform gates
    - d. All emergency gates at the stations, MSF Buildings and Yard
    - e. All access panels for automated external defibrillators
    - f. Blue light stations (BLS)
    - g. All Communication Cabinets
    - h. Communication Distribution Cabinets
  2. The IDS will detect and monitor alarm conditions and provide the required sensor equipment, local alarm annunciations and the corresponding Supervisory Control And Data Acquisition (SCADA) remote outputs. All detected alarms, and troubles will be transmitted to OCC via the Cable Transmission System (CTS) for recording.
  3. The intrusion alarm equipment will be compatible with, and capable of interfacing to the City's SCADA system.
- B. Section Includes:
1. General
  2. Preparation
  3. Naming
  4. Delivery, Storage and Handling
  5. Installation
  6. Testing and Inspection
  7. Training
- C. Related Sections:
1. Section 28 13 00 – Access Control System

## **1.02 PRICE AND PAYMENT PROCEDURES**

- A. General: Separate measurement of payment will not be made for the Work required under this Section. All costs in connection with the Work specified herein will be considered to be included with the related item of work in the General Conditions, or incidental to the Work.

## **1.03 CODES, STANDARDS AND RECOMMENDED PRACTICES**

- A. The governing version of the listed documents shall be the latest as adopted and administered by the City.
- B. Federal Communications Commission (FCC):
  - 1. 47 CFR 15 Radio Frequency Devices
- C. Institute of Electrical and Electronic Engineers (IEEE):
  - 1. IEEE 730 Software Quality Assurance Plans
  - 2. IEEE 1012 Software Verification and Validation Program
  - 3. IEEE C37.1-1994 IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control
- D. National Electrical Manufacturers Associations (NEMA):
  - 1. NEMA 250 Enclosures for Electrical Equipment (1000 Volts Maximum)
- E. Underwriters Laboratories, Inc. (UL):
  - 1. UL 1076 Proprietary Burglar Alarm Units and Systems
- F. National Fire Protection Association (NFPA):
  - 1. NFPA 70 National Electrical Code
- G. Applicable Federal, State, and Local Laws, Regulations, and Codes.

## **1.04 QUALITY ASSURANCE**

- A. General: Refer to General Conditions for quality assurance requirements and procedures.
- B. Quality Assurance Program: The manufacture, test and installation of the IDS shall conform to the requirements of the approved Quality Assurance Program and the Quality Assurance provisions of this Contract.
- C. The Contractor must employ factory-trained service personnel with a minimum of 5 years experience in servicing IDS related equipment.
- D. Comply with all applicable Federal, State, and Local Laws, Regulations, and Codes including those referenced in Article 1.03.

## 1.05 SYSTEM DESCRIPTION

### A. General:

1. The intrusion alarm system shall be electrically supervised, closed circuit, and continuously self-monitoring. System components shall conform to applicable codes and standards.
2. All intrusion and trouble alarms from each station and other facilities shall be transmitted to the local Intrusion Alarm control Panel (IACP) and to the OCC through the Local Area Network (LAN) and the CTS. Indications of deactivated detectors shall also be provided from each station and other facilities. Automatic recording of an intrusion indication, including a permanent record of date, time, and location, shall be provided at the OCC and archived. Provision shall be made to test the system locally and remotely.

### B. At-Grade and Aerial Stations: All enclosed spaces in at-grade and aerial stations shall be equipped with an intrusion alarm system to monitor doors as described in these specifications.

### C. System Design: The design of the Intrusion Alarm System (IAS) shall include the following major components.

1. Intrusion Alarm Control Panel: An Intrusion Alarm control Panel (IACP) shall be provided in a secured area adjacent to the station fire alarm control panel. The IACP shall contain all the logic and circuitry required to supervise and control the intrusion detectors. The IACP shall be modular in construction to provide for ease of maintenance and expansion. It shall contain trouble circuitry powered from a dedicated power source that electrically supervises all IAS circuit wiring for a "Short" or an "Open." The IACP shall perform the following functions:
  - a. Provide intrusion alarm detection
  - b. Provide trouble detection
  - c. Provide audible and visual "Trouble" and "Alarm" indications at the Intrusion Alarm Annunciator Panel (IAAP)
  - d. Provide common system controls to the IAAP
  - e. Provide input to the CTS to indicate "Alarm" and "Trouble" conditions
  - f. Indicate ac Power failure
  - g. Indicate battery voltage
  - h. Indicate battery charging current
2. Intrusion Alarm Annunciator Panel: An Intrusion Alarm Annunciator Panel (IAAP) shall be located in each passenger station at an accessible location and in proximity to Fire Alarm Annunciator Panel. The IAAP shall contain visual and audible alarm indicators associated with each device for "Alarm" and "Trouble" condition. The audible annunciator shall indicate alarm and a trouble conditions by using distinct tone.
3. Intrusion Detection System: The Intrusion Detection System (IDS) shall consist of intrusion detectors located in the passenger station rooms and equipment areas. Intrusion detectors shall provide alarms indicating unauthorized entry when a protected door is opened.

4. The activation of an intrusion detector at a station shall cause a display of an alarm indication at the station intrusion alarm control panel, identifying the location and devices at which the alarm condition exists. It shall provide additional outputs as follows:
    - a. To the CTS for transmission of intrusion signal to OCC
    - b. To an audible alarm outside the station when the station is closed
    - c. To the IAAP in the station
  5. The visual indication on IAAP shall remain until the detection system is reset, and the audible alarm shall continue until acknowledged at the panel, or the detection device is reset or disabled. The audible signal shall be restarted by any subsequent intrusion signal, whether the first detection device has reset or not. The audible alarm shall be separate from the audible alarm for the fire alarm system, and shall have a different sound frequency.
  6. A malfunction on any detector circuit or an input power failure shall cause a display on the station intrusion alarm control panel and IAAP of an indication identifying the detector circuit which has malfunctioned, or indicating an input power failure. It also shall cause an output to CTS in the facility for transmission to OCC. The visual indication shall remain until the malfunction is corrected. The audible signal shall continue until acknowledged at the IAAP and shall be restarted by subsequent malfunctions prior to correction of the initial malfunction.
  7. Entry Delay:
    - a. A delay circuit that allows entry into protected premises shall be limited to only those initiating devices, such as door contacts installed on entry doors, which must be bypassed to allow access to the mechanism that is used to place the system in a disarmed state.
    - b. The local and remote reporting of an intrusion shall not occur until after a pre-selected elapsed time has occurred. This time shall be adjustable from 10 seconds to 4 minutes and shall normally be set for 30 seconds. An "acknowledge" key-operated switch shall be provided. It shall cancel alarms if actuated.
    - c. A key-operated switch, or digital or other access control device at the entrance to each protected area within a station, shall be provided to disable the intrusion detection devices for that area. With a switch in the disable position, a visual indication shall be displayed at the IACP showing the protected area that is disabled. It also shall display disabled indication on the IAAP. This disable status shall also be transmitted to OCC.
    - d. The maximum interval of time between the opening of an entry door and reaching the mechanism that is used to disarm the system shall be no greater than one-half of the entry delay time programmed for the system.
- D. Roll-up Grilles at Passenger Station Entrance:
1. Roll-up doors at the station entrance shall have door position indicators and audible alarms. The interior and exterior junction box associated with each door or gate shall house the audible alarm and key switch.
  2. In order to open these doors without transmitting an intrusion alert and simultaneously activating the associated audible alarm, an alarm bypass control

shall be provided. The bypass control shall be housed in a separate and distinct intrusion alarm junction box and shall be operated by the key switch. Actuation of the key switch shall nullify all the individual audible alarms and the intrusion alert for as long as the key switch is in the bypass position and a light shall indicate that the system is in bypass.

3. The junction box in the protected space shall be provided with alarm ON, OFF and Silence controls.

E. Maintenance and Storage Facility:

1. The activation of an intrusion detector in a Maintenance and Storage Facility (MSF) buildings, and designated offices shall sound an audible alarm in the protected area and cause a display of an alarm indication at the intrusion alarm control panel in the OCC and at the intrusion alarm annunciator panel in the facility guard office showing the device and location in which the alarm condition exists. The audible alarm and visual indication shall continue until acknowledged at the panel or the detection device is reset or disabled. The audible alarm shall have a different sound from that indicating a fire.
2. At the entrance to each protected area key operated switches shall be provided to disable the intrusion detection devices for the location. With a switch in the disable position, a visual indication shall be displayed at OCC and at the intrusion alarm annunciator panel in the facility guard office showing the device and location that is disabled.
3. The entry delay shall be as defined above.

- F. Wayside Miscellaneous Rooms: Entry gates at wayside traction power substation (TPSS) and GBS sites shall have intrusion alarm systems. Electro-mechanical intrusion detection devices shall be provided on each gate and hinged access pane. The detection devices shall actuate upon opening of the gate by any means. All intrusion and trouble alarms shall be transmitted to OCC through SCADA PLC using CTS and FOCN. Means shall be provided to deactivate the intrusion detectors from OCC or through the local keyed switch.

- G. Fare Vending Equipment: The Fare Vending Equipment shall be equipped with intrusion detectors. These intrusion detectors shall be combined so that each fare vending equipment array in each station is one intrusion zone. The design shall interface with the Fare Vending Equipment system design. All intrusion and trouble alarms shall be transmitted to IACP and OCC through CTS and FOCN.

## 1.06 SUBMITTALS

- A. General: Refer to the General Conditions for submittal requirements and procedures.
- B. Provide system descriptive information, manufacturer's product descriptions, catalog data and information.
- C. Provide a Deployment Diagram that includes all types of logical devices and software used to detect and report intrusion alarms. Include PLCs, network processors, computers, software and databases.

- D. Provide architecturally scaled floor plan drawings showing the location of all rooms, cabinets, or areas that are monitored for intrusion detection. Drawings used for the ACS design submittal, Section 28 13 00 – Access Control System, may be reused for ACS controlled doors.
1. Point-to-point wiring diagrams: Indicating terminal-to-terminal connection between system components, type of connections, and other information necessary to make final terminations.
  2. Identify all doors that are monitored for intrusion on the same intrusion circuit.
  3. Show equipment locations and cable routing and wiring in conduits, raceways and cable trays.
  4. Indicate cable types and sizes, routing, splice and connection points, equipment locations, and equipment ID names.
  5. For all identification of equipment on drawings, use the standard convention in general use for all communications and IDS equipment.
- E. Battery calculations: Provide standby current requirements, quantity and type of batteries proposed, and calculated standby time under normal and worst-case operating conditions.
- F. Final User Documents: Prior to Final Acceptance Testing, submit final versions of the following:
1. User Manuals.
  2. Maintenance Manuals, with spare part list.
  3. Manufacturer's installation instructions.
  4. Shop Drawings: Indicating actual device placements, number and type of wires and cables between devices, equipment mounting details, power requirements, data circuit requirements, point numbers, and equipment addresses, and site and building floor plans showing conduit size and routing.
  5. Final Acceptance Test Procedure: Prior to the Final Acceptance Test, submit the Final Acceptance Test procedure.
  6. Test Results: Prior to acceptance of the intrusion detection system, all test results must be submitted for approval.
  7. A backup copy of the latest software programmed in the Control Unit shall be submitted to the City in a Compact Disk (CD) or DVD format with software revision number clearly labeled, and dated. Relinquish all passwords programmed in the Control Unit to the City upon final acceptance test.
  8. Training Manuals.
  9. Training Plan.
  10. Course outlines for each of the end user training programs. The course outlines shall include the course duration, and a brief description of the subject matter.

## **PART 2 – PRODUCTS**

### **2.01 GENERAL**

- A. All equipment and components shall be new, and the manufacturer's current model. The materials, appliances, equipment and devices shall be tested and listed by a nationally recognized approval agency for use as part of an intrusion detection system. The authorized representative of the manufacturer of the major equipment, such as control panels, shall be responsible for the satisfactory installation of the complete system.
- B. All equipment and components shall be installed in strict compliance with each manufacturer's recommendations. Consult manufacturer's installation manuals for all wiring diagrams, schematics, physical equipment sizes, etc. before beginning system installation.
- C. Intrusion detection shall be provided, as a minimum, for the following locations:
  - 1. Train Control and Communications rooms
  - 2. Electrical equipment rooms
  - 3. Elevator equipment rooms
  - 4. Battery rooms
  - 5. Mechanical/Fan rooms
  - 6. Station entrance roll-up-grilles
  - 7. Traction Power Substations site gate
  - 8. Gap Breaker Stations site gate
  - 9. Station emergency exits
  - 10. Station end-of-platform gates
  - 11. Access to non public areas from station public areas
  - 12. Access panels for automated external defibrillators
  - 13. Blue light stations
  - 14. Ticket vending machines
  - 15. Communication Cabinets
  - 16. Storage room in MSF
  - 17. Other selected rooms in MSF buildings
- D. Various types of intrusion detectors shall be installed to detect unauthorized access into a monitored area. The IDS shall detect unauthorized intrusions that shall be alarmed and reported to OCC.
  - 1. ACS Controlled Doors: All doors controlled by ACS card keys shall report intrusion alarms as detected by the ACS gate controllers. Devise an effective

method for modifying the loops to alarm each door. See Section 28 13 00 – Access Control System.

2. **Intrusion Alarm Monitored Areas:** Upon detection of an intrusion at the intrusion alarm monitored doors, end-of-platform gates, emergency exit gates at stations, ticket vending equipment and access panels for automated external defibrillators and blue light stations the intrusion detection system shall produce an alarm at the local station processing equipment. The local station processing equipment shall provide for temporary storage, processing, and transmission of the alarm to the local alarm annunciator panel system and to the main intrusion detection CPU at OCC through SCADA.
3. **Cabinet Intrusion Detection:** A circuit that detects when the cabinet door is open shall be installed to protect all Communications Cabinets containing SONET or Ethernet network communications. Whenever the cabinet door is opened, an alarm shall be generated.

## **2.02 EQUIPMENT**

- A. **Gate Controllers:** Gate controllers are part of the Access Control System specified in Section 28 13 00 – Access Control System. The gate controller shall generate intrusion alarms from the magnetic contact switch inputs on the door or gate.
- B. The IDS equipment at OCC shall be comprised of the following major components:
  1. Video display terminal
  2. Central Processing Unit
  3. Printer
  4. Intrusion detection rack
- C. **Intrusion Alarm Control Panel:** Subject to compliance with requirements specified herein, provide the product by an approved manufacturer.
- D. **Intrusion Alarm Annunciator Panel:** Subject to compliance with requirements specified herein, provide the product by an approved manufacturer.
- E. **Magnetic Contact Switches:**
  1. On access controlled doors magnetic contact switches shall be provided under Section 28 13 00 – Access Control System. Additional magnetic contact switches shall be installed on doors that are not ACS controlled. Determine the materials and methods for each door for an inconspicuous installation. Contact closures shall be wired singly or to a nearby Gate Controller for PLC discrete input.
  2. The magnetic switch shall consist of flush mounted magnet and switch assemblies, each housed in thermoplastic.
  3. The switch assembly shall activate when the magnet is more than 1/4-inch removed.
  4. Normally open and normally closed contacts shall be provided.
  5. All intrusion contacts shall be monitored by using a supervised loop.

6. The magnetic switch provided shall be capable of a minimum of 100,000 operations over a minimum period of 10 years without failure.
- F. Tamper Switches: Tamper switches shall cause activation of alarms whenever the door of an enclosure is opened. Tamper switches shall be recessed plunger switches with closed-loop contacts. Provide mounting brackets and other miscellaneous hardware to mount to panels and within enclosures. Tamper switch shall be selected as required to suit conditions.
- G. Detectors Wiring: Fully supervised Class-A circuits shall be utilized for activation of alarm indication from sensors (switches) to control panel.
- H. Alarm Bell:
1. Alarm bells shall be fabricated from a high quality die casting with a baked red enamel finish.
  2. Power consumption shall be 0.030 ampere at 24V DC.
  3. Typical output shall be 84 dBa at 24V DC.
  4. Typical output shall not be less than 15 dBa above ambient noise level.
  5. Alarm bells shall mount to a standard 4-inch square outlet box.
- I. Enclosures: All control equipment, relays, modules, circuit boards and other such devices shall be contained within enclosures of all-metal construction. All enclosures shall be closed with tamper resistant screws. Provide NEMA enclosures for all equipment that is not provided by the manufacturer in a suitable enclosure. The intrusion alarm control unit shall be housed in a NEMA-I2 enclosure with locking cover. Front panel Light Emitting Diode (LED) indications shall be provided for power on and battery status.
- J. Power Supplies and Batteries:
1. Intrusion Alarm equipment shall receive primary power from the Main AC Power Distribution panel.
  2. Transfer from normal to Emergency power or restoration from emergency to normal power shall be fully automatic and shall not prevent transmission nor cause false transmission of an alarm.
  3. The Intrusion Alarm Control Panel shall be installed with an individual battery backup system, for 48 hours of battery-power operation.
  4. Battery wiring harness shall be provided as needed to properly connect batteries to power supply.
  5. Power supplies shall be provided with dry contact relay that opens upon power fault. Power supply power fault shall be managed as an alarm by the OCC.
- K. Wire and Cable:
1. Provide cabling between all intrusion detection components in accordance with manufacturer's requirements. All cabling shall be shielded unless otherwise specified by manufacturer.

2. Comply with equipment manufacturer's recommendations for wire and cable.
- L. Miscellaneous Equipment: Furnish and install miscellaneous equipment to complete the IDS. This shall include surface conduit between electrical junction boxes and IDS devices, and miscellaneous mounting hardware.

### **2.03 INTRUSION DETECTION SYSTEM MANAGEMENT SYSTEM**

- A. An Intrusion Detection System Management System shall be provided which permits configuration management, fault reporting and interfacing to other subsystems.
- B. IDS Management Software shall be developed to conform to the applicable IEEE standards for software development and quality assurance including but not limited to:
  1. IEEE 730: IEEE Standard for Software Quality Assurance Plans
  2. IEEE 1012: IEEE Standard for Software Verification and Validation
  3. IEEE Std C37.1-1994 - IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control

## **PART 3 – EXECUTION**

### **3.01 GENERAL**

- A. Provide all labor, tools, supplies, materials and equipment required for the design, installation, configuration, programming, and testing of the intrusion detection system.

### **3.02 PREPARATION**

- A. City will schedule design reviews with Contractor. The design reviews shall encompass all design submittals.

### **3.03 NAMING**

- A. Assign unique identification names to the major components and equipment used for intrusion detection. These identification names shall be used on submittal drawings.

### **3.04 DELIVERY, STORAGE AND HANDLING**

- A. Contractor is responsible for all delivery, storage, and handling of equipment.

### **3.05 INSTALLATION**

- A. Submit installation drawings prior to installation of intrusion detection components. Proceed with the installation only after the approval of installation drawings.
- B. Follow manufacturer's recommended installation practices, Specifications and RFP Plans during construction. The approved Installation design submittal shall be used for the physical installation of components necessary for intrusion detection system.
- C. All equipment shall be permanently attached to walls and ceiling / floor assemblies and shall be held firmly in place. Fasteners and supports shall be adequate to support the required load.

- D. Install all equipment, wire and conduit in accordance with manufacturer's recommendations, applicable codes and standards, and approved shop drawings.
- E. Furnish and install clamps or other cable-restraining hardware in areas where support is required for cables entering or leaving conduit.
- F. Cable entrance openings in equipment enclosures and junction boxes shall be sealed with compression-type fittings or pliable sealing compound after cable is in place. Sealing compound shall be used to seal area around cable where it emerges from the end of a conduit or junction boxes. The filling compound shall be applied in conformance with manufacturer's instructions.
- G. Wire or cable terminated on terminal equipment that is moveable (such as terminal blocks mounted on swivels) shall be routed to the terminal equipment such that, when the terminal equipment is rotated or moved, the wire or cable twists instead of bending.
- H. Cable terminations shall have permanent cable tags identifying the cable number, the number of copper pairs in the cable, the distant end (where the cable goes) and the route that it takes.
- I. Wiring Within Enclosures: Install conductors paralleled with or at right angle to the side and back of enclosure. Bundle, lace and train the conductors to terminal points with no excess. Connect conductors that are terminated, spliced, or interrupted in any enclosure associated with the IDS to terminal blocks. Mark each terminal in accordance with the wiring diagrams of the system. Make all connections with approved crimp-on terminal spade lugs, pressure-type terminal blocks, or plug connectors.

### **3.06 TESTING AND INSPECTION**

- A. Perform the following inspection and test on the Intrusion Detection System at each equipment installed location. The City shall be given at least 10 days written notice prior to each scheduled test so that the City may be present as desired.
  - 1. Factory Testing and Inspection: Factory testing and inspection of IDS shall include the following:
    - a. Each Intrusion alarm control panel shall be powered-up and tested after the factory wiring is complete.
    - b. Verify magnetic switch and alarm operation.
    - c. Verify intrusion alarm keypad operation.
  - 2. Field Inspection: Field Inspection of IDS equipment at each location shall include verification of the following;
    - a. Conformance to standards, methods, quality, specification requirements and approved drawings.
    - b. Proper routing and termination of wire and cable.
    - c. Secured cable and wire connections.
    - d. Proper grounding of all equipment
    - e. Correct and complete labeling and tagging of wire, cable, terminal, connectors and equipment.

3. Field Testing: The tests shall be performed in the presence of the City under the supervision of the intrusion alarm system manufacturer's qualified representative. The field testing shall include the following.
  - a. Provide all instruments and personnel required for the tests.
  - b. Subject the system to a complete functional and operational performance test.
  - c. Verify operation of the magnetic switches.
  - d. Measure audible alarms output level from specified locations.
  - e. Test all inputs, outputs, and functions of the Intrusion Alarm Control Panel.
  - f. Test all functions of the Intrusion Alarm Annunciation Panel.
4. System Acceptance Test: The tests shall include the following:
  - a. Tests to indicate there are no grounded, shorted, or open circuits.
  - b. Tests of each input to the Intrusion Alarm Control Panel, including transmission of trouble and alarm signals across local PLC at each location and to OCC.
  - c. Tests of normal and emergency power supplies, including batteries.

### **3.07 TRAINING**

- A. A minimum of four members of staff must receive sufficient training on the operation and configuration of the system to enable these operators to train others. The training shall be conducted by the manufacturer's own training staff or by other certified training staff.
- B. Self-training materials shall be available for the software user interface.

**END OF SECTION**