SECTION 13700

DETECTION AND ALARM

B9512G and B8512G Alarm Systems

Display hidden notes to specifier. Word 2003 (or earlier): "Tools" "Options" "View" "Hidden Text"     Word 2007:Click on Office logo (upper left corner); Click on Word Options (bottom right); Left menu, click on Display; Under "Always show these" select "Hidden Text"

\*\* NOTE TO SPECIFIER \*\* Bosch Security Systems; systems for video surveillance, access control, and intrusion and fire detection.  
  
This section is based on the products of Bosch Security Systems, which is located at:  
130 Perinton Pkwy.   
Fairport, NY 14450  
Toll Free Tel: 800-289-0096  
Tel: 585-223-4060  
Email: [request info (presales.support@us.bosch.com)](http://admin.arcat.com/users.pl?action=UserEmail&company=Bosch%20Security%20Systems&coid=44833&rep=&fax=&message=RE:%20Spec%20Question%20(13700bss):%20%20&mf=)  
Web: [www.boschsecurity.us](http://www.boschsecurity.us)   
[ Click Here ] for additional information.

For Europe:

**Bosch Security Systems B.V.**

**Torenallee 49**

**5617 BA Eindhoven**

**The Netherlands  
Phone: + 31 40 2577 284**

[**emea.securitysystems@bosch.com**](mailto:emea.securitysystems@bosch.com)

[**www.boschsecurity.com**](https://www.boschsecurity.com/xc/en/)

Bosch Security Systems, Inc. works closely with an extensive network of certified dealers and integrators to design dependable security and life safety solutions for the market. Our broad portfolio of products and systems for video surveillance, access control, and intrusion and fire detection are used by major schools and universities, government agencies, correctional facilities, retail stores, casinos and in many other commercial environments throughout North America.  
   
Our significant investment in research and development is unsurpassed in the security industry and enables us to regularly update our existing products and introduce new technologies. These advancements are continually recognized by the market. For example, the products we manufacture for networked video systems have won 11 awards in the last three years. Our solution for integrating building security and management systems across an enterprise has been implemented by various Fortune 500 companies and can facilitate centralized management of an organization's assets. Testing by independent certified regulatory compliance organizations verifies updates to our intrusion and fire systems extend beyond minimum compliance requirements. And, while technological innovation is important, we ensure that new product development addresses all the concerns paramount in the world of security and life safety today, including performance, quality, and ease of installation, maintenance and use.  
   
For more than 125 years, the Bosch name has stood for quality and reliability. We are there for our customers during all crucial phases of a project: before, during and after the sale.

1. GENERAL
   1. SECTION INCLUDES
      1. Integrated Digital Alarm Communicator and Access Control System (DACS), including but not limited to the following:
         1. Control panel.
         2. Enclosures.
         3. Lock and key.
         4. Power Supplies.
         5. Accessories required to provide a complete DACS.
         6. System O and I manual.
         7. System programming.
         8. Batteries.
         9. Wiring.
         10. Conduits.
      2. The Contractor shall be responsible for identifying requirements for permits from the local police department for the installation of the alarm system specified herein and shall assist the Owner in obtaining the relevant alarm permits.
   2. RELATED SECTIONS

\*\* NOTE TO SPECIFIER \*\* Delete any sections below not relevant to this project; add others as required.

* + 1. Section 16050 - Basic Electrical Methods and Materials: Intrusion detection systems Infrastructure.
    2. Section 13703 - Access Control.
    3. Section 13800 - Building Automation and Control.
  1. SYSTEM DESCRIPTION

\*\* NOTE TO SPECIFIER \*\* Delete any items below not applicable to this project; add others as required.

* + 1. A functionally complete, integrated Digital Alarm Communicator System (DACS) per manufacturer's guidelines, codes and specification requirements.
       1. The DACS shall include a Control Panel with built-in Ethernet jack for event communication and remote services.
       2. The DACS shall include a Control Panel with an optional, supervised telephone line interface module.
       3. The DACS shall include recording and retention of event information in a dedicated event log.
       4. The DACS shall incorporate an integral real-time clock, calendar, and a test timer.
       5. The DACS shall incorporate battery charging capabilities with supervision of battery voltage and battery leads.
       6. The DACS shall accommodate a time / event-based scheduling system.
       7. The DACS shall be capable of supervision of peripheral devices and communications interfaces.
       8. The DACS shall accommodate configuration and operation of separate, independent areas.
       9. The DACS shall accommodate hard-wired or wireless point expansion via eight-point interface modules and RF receivers.
       10. The DACS shall accommodate addressable expansion utilizing a 2-wire bus
       11. the DACS incorporate removable terminal strips for wiring connection to facilitate simple service and replacement
       12. The DACS shall have electrically supervised detection loops and power supplies with battery(s) maintenance. This supervision shall be programmable for the purposes of reporting this information to the DACR.
       13. The DACS shall be capable of sending (manually or automatically) test and status reports to remote DACRs.
       14. The DACS shall be able to accommodate test, diagnostics, and configuration programming functions locally or remotely via a portable programmer or a computer running the Remote Programming Software (RPS).
       15. The DACS shall annunciate alarm, trouble, service reminders, and other relevant system status messages in custom English, Latin American Spanish, Portuguese, Canadian French, Hungarian, Greek, Italian, Polish, German, Dutch, Swedish and/or Chinese text at the ACC.
  1. REFERENCES

\*\* NOTE TO SPECIFIER \*\* Delete references from the list below that are not actually required by the text of the edited section.

* + 1. National Electric Code, Article 760.
    2. National Fire Alarm Code (NFPA 72).
    3. Administrative Council for Terminal Attachments (ACTA):
       1. ANSI/TIA-968-A-2002 Technical Requirements for Connection of Terminal Equipment to the Telephone Network.
    4. American National Standards Institute (ANSI):
       1. ANSI C63.4 Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz.
    5. California State Fire Marshal (CSFM):
       1. Title 19, California Code of Regulations, Building Material Listing Program (BML).
    6. Federal Communications Commission (FCC):
       1. Title 47 C.F.R. Part 15; Class B – Radiated and Conducted Emissions.
       2. Title 47 C.F.R. Part 68; rules governing the connection of Terminal Equipment (TE) to the Public Switched Telephone Network (PSTN).
    7. The National Institute of Standards and Technology of the United States of America (NIST):
       1. Federal Information Processing Standards Publications 197 (FIPS 197) –Advanced Encryption Standard (AES).
    8. International Organization For Standardization (ISO):
       1. 9001 - Quality System.
    9. Underwriters Laboratories, Inc. (UL):
       1. UL 50 - Enclosures for Electrical Equipment.
       2. UL 294 – Access Control System Units.
       3. UL 365 - Police Station Connected Burglar Alarm Units and Systems.
       4. UL 609 - Local Burglar Alarm Units and Systems.
       5. UL864 – Control Units and Accessories for fie Alarm Systems (Commercial Fire)
       6. UL 985 - Household Fire Warning System Units.
       7. UL 1023 - Household Burglar Alarm System Units.
       8. UL 1076 – Proprietary Burglar Alarm Units and Systems
       9. UL 1610 - Central Station Burglar-Alarm Units.
       10. UL 60950-1 - Information Technology Equipment - Safety.
       11. UL 636 – Hold up alarms
    10. Canada
        1. CAN/ULC S304 - Signal Receiving Centre and Premise
        2. CAN/ULC S545 - Residential Fire Warning System Control
        3. ICES-003 – Information Technology Equipment (ITE)
        4. ULC-ORD C1023 - Household Burglar Alarm System Units
        5. ULC-ORD C1076 - Proprietary Burglar Alarm Units and System
    11. Europe
        1. CE EMC, LVD, RoHS [B9512G, B9512G-E,B8512G, B8512G-E]

\*\* NOTE TO SPECIFIER \*\* Delete submittal requirements not required.

* 1. SUBMITTALS
     1. Submit under provisions of section 01300.
     2. Product Data: Manufacturer's data, user and installation manuals for all equipment and software programs including computer equipment and other equipment required for complete Digital Alarm including:
        1. Preparation instructions and recommendations.
        2. Storage and handling requirements and recommendations.
        3. Installation methods.
     3. Shop Drawings: Shop drawings shall provide details of proposed system and the work to be provided. Include point-to-point drawings of systems and wiring diagrams of individual devices.
        1. Detailed wiring diagrams and system description.
        2. System device locations on architectural floor plans.
        3. Full Schematic of system, including wiring information for all devices.
     4. Documentation to be submitted by the Contractor upon completion of system installation:
        1. "As-builts": Upon completion of installation, the Contractor shall prepare "as-built" drawings of the system. These "As-builts" shall be 30 inches by 42 inches (76 cm by 107 cm) format mylar reproducible drawings of each floor plan indicating exact device locations, panel terminations, cable routes and wire numbers as tagged and color-coded on the cable tag.
           1. Additionally, final point-to-point wiring diagrams of each type of device (on 30 inches by 42 inches (76 cm by 107 cm) format) shall be included in the "as-builts."
           2. "As-builts" shall be submitted to the Owner for approval prior to the system acceptance walk-through.
        2. Operation and maintenance manuals: Three sets of operating manuals shall be provided explaining the operation and maintenance of the system.
        3. Parts list.
        4. Maintenance required and maintenance schedule.

\*\* NOTE TO SPECIFIER \*\* Delete selection samples if colors have already been selected.

* + 1. Selection Samples: For each finish product specified, two complete sets of color chips representing manufacturer's full range of available colors and patterns.
    2. Verification Samples: For each finish product specified, two samples, minimum size 6 inches (150 mm) square, representing actual product, color, and patterns.
  1. QUALITY ASSURANCE
     1. Manufacturer Qualification:
        1. The system shall be the standard product of one manufacturer, and the manufacturer shall have been in business manufacturing similar products for at least 5 years.
        2. Manufacturer's Quality System: Registered to ISO 9001:2000 Quality Standard.
     2. Installer Qualification:
        1. Minimum of five years experience installing access control, surveillance and security systems and devices.
        2. After-sales support: The Contractor shall be a factory-authorized and trained dealer of the system and shall be factory-trained and certified to maintain/repair the system after system acceptance.
     3. System Requirements:

\*\* NOTE TO SPECIFIER \*\* Delete listing agency not required.

* + - 1. All equipment, systems, and materials furnished and installed under this section shall be installed in accordance with the applicable standards of:
         1. National Codes: NEC, NFPA, UBC, BOCA, SBCCI, IBC, as applicable.
         2. Approvals and listings: UL, ULC, FM, ANSI SIA CP-01, CSFM, NYC-CoA, as applicable.
         3. Local Authorities Having Jurisdiction (AHJ).

\*\* NOTE TO SPECIFIER \*\* Include a mock-up if the project size and/or quality warrant taking such a precaution. The following is one example of how a mock-up on a large project might be specified. When deciding on the extent of the mock-up, consider all the major different types of work on the project.

* + 1. Mock-Up: provide a mock-up for evaluation of installation techniques and application workmanship.
       1. Finish system in areas designated by Architect.
       2. Do not proceed with remaining work until workmanship and aesthetics are approved by Architect.
       3. Remake mock-up area as required to produce acceptable work.
  1. DELIVERY, STORAGE, AND HANDLING
     1. Deliver materials in manufacturer's original, unopened, undamaged containers; and unharmed original identification labels.
     2. Store products in manufacturer's unopened packaging until ready for installation.
     3. Protect store materials from environmental and temperature conditions following manufacturer's instructions.
     4. Handle and operate products and systems according to manufacturer's instructions.
  2. PROJECT CONDITIONS
     1. Maintain environmental conditions (temperature, humidity, and ventilation) within limits recommended by manufacturer for optimum results. Do not install products under environmental conditions outside manufacturer's absolute limits.
  3. WARRANTY

\*\* NOTE TO SPECIFIER \*\* Refer to manufacturer's literature for warranty provisions.

* + 1. All components, parts, and assemblies supplied by the manufacturers and installed by the Contractor shall be warranted against defects in material and workmanship for a period of at least 12 months (parts and labor), commencing upon date of acceptance by Owner. A qualified factory-trained service representative shall provide warranty service.
    2. Service/Maintenance:
       1. System maintenance and repair of system or workmanship defects during the warranty period shall be provided by the Contractor free of charge (parts and labor).
       2. Periodic testing of the system shall be carried out on a monthly or quarterly basis to ensure the integrity of the control panel, the sensing devices, and the telephone lines.
       3. The installer shall correct any system defect within six hours of receipt of call from the Owner.
       4. Extended service/maintenance agreements shall be offered by the Contractor for up to four years after the warranty expires. The agreement shall be renewable monthly, quarterly, or yearly.

1. PRODUCTS
   1. MANUFACTURERS
      1. Acceptable Manufacturer:
         1. North America: Bosch Security Systems, Inc.; 130 Perinton Parkway; Fairport, NY 14450. ASD. Toll Free Tel: 800-289-0096. Tel: 585-223-4060. Email: [request info (presales.support@us.bosch.com)](http://admin.arcat.com/users.pl?action=UserEmail&company=Bosch%20Security%20Systems&coid=44833&rep=&fax=&message=RE:%20Spec%20Question%20(13700bss):%20%20&mf=). Web: [www.boschsecurity.us](http://www.boschsecurity.us).
         2. Europe: Bosch Security Systems B.V.; Torenallee 49; 5617 BA Eindhoven; The Netherlands; Phone: + 31 40 2577 284; [emea.securitysystems@bosch.com](mailto:emea.securitysystems@bosch.com); [www.boschsecurity.com](https://www.boschsecurity.com/xc/en/)

\*\* NOTE TO SPECIFIER \*\* Delete one of the following two paragraphs; coordinate with requirements of Division 1 section on product options and substitutions.

* + 1. Substitutions: Not permitted.
    2. Requests for substitutions will be considered in accordance with provisions of section 01600.
  1. GENERAL DESCRIPTION
     1. Control Panel and Features:

\*\* NOTE TO SPECIFIER \*\* Select applicable control panel. Delete others.

* + - 1. The DACS control panel shall be Bosch Security Systems, Inc. model B9512G comprising a fully integrated intrusion and residential fire control system. The control panel shall support the following:
         1. The DACS system is capable of being utilized as a combination Intrusion and Commercial Fire system per code. Fully integrated intrusion and fire functions allow users to interface with 1 system instead of 2
         2. Optional Telephone Line Module, programmable for signaling and supervision.
         3. Integrated Conettix IP based communication provides high-speed, secure alarm transport and control.
         4. 32 programmable areas with perimeter and interior partitioning.
         5. 8 on-board, hardwired points with expansion capability for a total of 599 using a combination of wired or wireless points.
         6. Compatibility with Color Graphic Touch Screen, 2-line alpha numeric capacitive touch, ATM style LCD or 2-line LCD style Alarm Keypads.
         7. Local or remote programming, test, and diagnostic capability via a computer running the Remote Programming Software (RPS).
         8. The system shall include an integrated USB port for local programming and diagnostics using a computer running Remote Programming Software (RPS) and a male USB2.0 to male USB 2.0 cable with no additional hardware modules required.
         9. The system shall support the use of an Apple iOS device and/or Android device for control. Functions to include arming, disarming and control of outputs and access door, viewing of connected IP cameras. This application shall connect directly to the DACS using internet, wifi or cellular communications and shall not require a third party server of network operations center (noc).
         10. The DACS will allow integration with up to 16 Bosch IP video cameras using the built-in Ethernet connection, allowing the cameras to act as inputs and outputs.
         11. The DACS shall support integration with the Bosch Video Management System (BVMS) using the built-in Ethernet adapter.
         12. The DACS shall support up to thirty-two (32) custom functions allowing the installer to combine up to 6 functions into one command. These custom functions shall be operated by keypad command, point activation, keyfob button, or programmable schedule
         13. The DACS shall support up to 32 keypad shortcuts which allow the installer to define which commands are available at each keypad.
         14. The system shall offer multiple language support that can be assigned per keypad. The system shall offer multiple language support that can be assigned per keypad. Languages supported must include English, Latin American Spanish, Portuguese, Canadian French, Hungarian, Greek, Italian, Polish, German, Dutch, Swedish and/or Chinese.
         15. The DACS shall support flash firmware upgrades of systems firmware for the control panel and peripherals, allowing for future updates.
         16. Integrated real time clock, calendar, test timer and programmable scheduling capability for relay control and automatic execution of system functions based on a time / event.
         17. Provide 1.4 amps of power for standby operation and 2.0 amps of alarm power, both rated at 12 VDC.
         18. 3 configurable form ‘C’ wet or dry-contact relay outputs with expansion capability for up to an additional 472 dry-contact relay outputs.
         19. Integrated battery charger with reverse hook up protection, battery supervision and battery deep discharge protection.
         20. Supervision of peripheral devices and communications interface(s).

\*\* NOTE TO SPECIFIER \*\* Expansion Points are optional. Delete if not required.

* + 1. Point Functionality and Expansion:
       1. Each point in the system shall be programmable to provide the following type of response in the system:
          1. Always on (24 hour response).
          2. On when the system is Master Armed.
          3. Only on when the system is Perimeter Armed.
          4. Displays / Does Not Display at the ACC when the point is activated.
          5. Provides / Does Not Provide entry warning tone.
          6. Sounds / Does Not Sound audible alarm indication.
          7. The Point is bypassable / not bypassable.
          8. Alarm Verification with programmable verification time.
          9. Fire Alarm Point
          10. Relay activation by Point.
          11. Provides / Does Not Provide "watch point" capability.
          12. Provides Swinger Bypass.
          13. Defers Bypass Report.
          14. Can return to the system after being force armed and then restoring.
          15. Can return to the system after being bypassed and then restoring.
          16. Keyswitch arming (maintained or momentary)
          17. Activate by Custom Function
          18. Activate following an output
          19. Gas Alarm
       2. The system shall support a programmable Monitor delay functionality for supervision of points during disarmed periods. These points may be programmed to ignore status from 1 to 60 minutes and will activate only if the point is off-normal for this time period.
       3. The system shall support a programmable delay response functionality for supervision of points during armed or disarmed periods. These points may be programmed to ignore status from 1 to 60 minutes and will activate only if the point is off-normal for this time period.
       4. The system shall support virtual points and outputs for customized programming of events
       5. The DACS shall be capable of supporting "group zoning." Group zoning refers to the combining of points into a separately identifiable and separately annunciated (programmable text) areas.
       6. The DACS shall be capable of allowing variable point response times via programming. Point response times shall be programmable over a range of 300 milliseconds to 4.5 seconds.

\*\* NOTE TO SPECIFIER \*\* B9512G. Delete if not required.

* + - 1. The DACS shall have the capability to expand up to 599 separately identifiable points, of which 8 are on-board and 472 are off-board wired, addressable or wireless points.
         1. The 8 on-board points shall be able to accommodate powered class B functionality using a powered loop interface module.
         2. Point Expansion Modules (Wired and Wireless) shall be able to be located remote to the main panel to a maximum distance of 1000 feet.
         3. Addressable modules shall be able to be located remote to the panel to a maximum of 500 feet.

\*\* NOTE TO SPECIFIER \*\* B9512G. Delete if not required.

* + - 1. The DACS shall have the capability to expand up to 99 separately identifiable points, of which 8 are on-board and 91 are off-board addressable points connected to multiplexed backbone trunks via wired modules and/or wireless receivers.
         1. The 8 on-board points shall be able to accommodate powered class B functionality using a powered loop interface module.
         2. Point Expansion Modules (Wired and Wireless) shall be able to be located remote to the main panel to a maximum distance of 1000 feet.
         3. Addressable modules shall be able to be located remote to the panel to a maximum of 500 feet.
    1. Areas/Accounts:

\*\* NOTE TO SPECIFIER \*\* B9512G. Delete if not required.

* + - 1. The DACS shall support 32 independent areas. Each of the 32 areas shall have custom text associated with the armed state, disarmed state and point-off-normal state.
      2. The DACS shall be capable of assigning 1 to 4 account identifiers to the areas depending on the distribution of areas per account.
      3. The DACS shall be capable of assigning 1 to 2 account identifiers to the areas depending on the distribution of areas per account.
      4. All of the areas must be capable of Master (All) and/or Perimeter (Part) arming (excluding predefined Interior protection).
      5. The DACS shall be capable of logically grouping 1 or more points into an area, or conversely, dividing 2 or more points into two or more areas.
      6. Any area shall be configurable to allow arming by specific users when a programmable number of devices are faulted or bypassed.
      7. Areas shall be independently controlled by their corresponding ACC.
      8. Area(s) shall accommodate assignment of independent account numbers to define annunciation, control, and reporting functions.
      9. The DACS shall be capable of linking multiple areas to a shared area which may be automatically controlled (hallway or lobby).
      10. The DACS shall accommodate conditional area arming dependant on the state of other areas (master or associate). Any area can be configured for perimeter and interior arming, not requiring a separate area for this function.

\*\* NOTE TO SPECIFIER \*\* Output Relay Expansion is optional. Delete if not required.

* + 1. Output Relay Expansion: The DACS shall provide the capability for output relay expansion using relay expansion modules. Independent control of relay functions by area shall be possible through programming assignments.

\*\* NOTE TO SPECIFIER \*\* B9512G. Delete if not required.

* + - 1. The DACS shall be capable of activating 472 additional relay outputs for auxiliary functions based on its classifications (area vs. panel wide). Output Expansion Modules shall be able to be located remote to the main panel to a maximum distance of 1000 feet. 8 relays (Form C) are to be provided per octo-relay module

\*\* NOTE TO SPECIFIER \*\* B8512G. Delete if not required.

* + - 1. The DACS shall be capable of activating 64 additional relay outputs for auxiliary functions based on its classifications (area vs. panel wide). Output Expansion Modules shall be able to be located remote to the main panel to a maximum distance of 1000 feet. 8 relays (Form C) are to be provided per octo-relay module
      2. The DACS shall be capable of controlling relays and automatically executing system functions based on a time / event scheduling program. The program can be hour, day of week or day of month based.
      3. Relays and other outputs may be programmed to follow up to 14 different area conditions or up to 12 panel conditions. Relays may also be programmed to follow individual points or groups of points.
      4. The DACS shall support 5 different types of alarm output selections: Steady, Pulsed, California Standard, Temporal Code 3 and Temporal Code 4.
    1. Scheduling: The DACS shall support scheduling capabilities with the following characteristics:
       1. Arm / Disarm specific area(s) based on open/close windows.
       2. Bypass / Unbypass point(s).
       3. Activate / Deactivate relay(s).
       4. Send test reports.
       5. Up to 4 programmable holiday schedules of 366 days each (includes leap year). Based on the holiday settings, different time windows for open/close and other system functions can be executed.
       6. Automatic adjustment of system clock for daylight savings time.
    2. Alarm Keypads:
       1. The DACS shall accommodate connection with up to 32 ACCs, each capable of displaying custom English, Latin American Spanish, Portuguese, Canadian French, Hungarian, Greek, Italian, Polish, German, Dutch, Swedish and/or Chinese text on a liquid crystal display.

\*\* NOTE TO SPECIFIER \*\* Delete if not required.

* + - 1. The Alarm Keypads shall accommodate viewing and configuration of system parameters including:
         1. Network Parameters:

DHCP Enable/Disable for the selected network module.

UPnP Enable/Disable for the selected network module.

IP Address for the selected network module

Subnet Mask for the selected network module.

Default Gateway for the selected network module.

Port Number for the selected network module - The module's port number shall range from 0 to 65,535.

DNS Server Address for the selected module's DNS server IP address

DNS Host Name for the selected module. The DNS host name shall contain up to 63 characters.

AES Encryption Key Size – Enable/Disable encryption by selecting the AES encryption key size for the selected network module.

AES Encryption Key String - The user shall be able to display, add and modify the AES encryption string based upon the key size previously configured for the selected network module.

* + - * 1. Point Parameters:

Point Selection between one and the maximum number of points in the control panel.

Point Registration to allow system response from a specific physical point on any one of the expansion modules; On-board or Point expansion modules (wired or wireless)

Wireless points shall be able to be enrolled in the system via an auto enrollment feature.

* + - * 1. Event Routing Parameters to allow programming of up to 4 report routing groups as well as configuration of primary and secondary paths.
    1. User Passcodes and Authority: Passcodes shall be programmable with authority levels to allow users to operate any or all areas.

\*\* NOTE TO SPECIFIER \*\* B9512G, Delete if not required.

* + - 1. Up to 2000 different passcodes shall be accommodated

\*\* NOTE TO SPECIFIER \*\* B8512G. Delete if not required.

* + - 1. Up to 500 different passcodes shall be accommodated.
      2. Each passcode shall be 3 to 6 digits (variable) and be assigned a 32-character user name
      3. User access to System features and functions shall be configurable based on 14 individually programmable levels of authority assigned to the user passcode. Additionally, the system shall have the capability to assign to the user passcode, a different authority level in each of the areas. A service passcode can be assigned to the servicing agent allowing the agent limited access to system functions. User-programmable / activated functions include:
         1. Arming the system: All areas, specific area(s) only, perimeter instant, perimeter delayed, perimeter partial, watch mode, and arming the system with a duress passcode.
         2. Disarming the system: All areas, specific area(s) only and disarming with a duress passcode.
         3. Viewing system status: Faulted points, event memory, bypassed points, area status and point status.
         4. Implementation functions: Bypass a point, unbypass a point, reset sensors, silence bell, activating relays, initiating the remote programming function locally to allow programming the system from a remote location.
         5. Testing the system: Local Walk test, Service Walk test, Fire test, send report to remote DACR to check the telephone link, and programming the time and date for the next test report transmission.
         6. Change system parameters: ACC display brightness, system time and date, and add/delete/change passcodes.
         7. Extend the closing time of the system.
         8. Transmitting special alerts and activating audible and visible signals.
         9. Executing multiple commands / ACC keystrokes from a single Menu / Command List item. This function shall be able to have a 32 character (alphanumeric) title to identify it on the ACC display.
         10. Editing of time / event based scheduling program from the ACC.
         11. The DACS shall also provide a "service menu" to implement functions such as viewing and printing the system log, displaying the system firmware revision number, and defaulting (toggling) text displays between custom and default text displays for troubleshooting.
      4. The DACS shall allow users to change their own user passcode from the Alarm Keypad (ACC). Managers shall be capable of changing the user passcodes and authority assignments by area of other users from the ACC.
      5. The DACS shall incorporate a programmable "Passcode Follows Scope" feature to allow users to arm or disarm only the area they are entering with one simple command or control all areas from one ACC.
    1. Access Control: THE DACS shall support access control using the B901 access control module(s).

\*\* NOTE TO SPECIFIER \*\* B9512G. Delete if not required.

* + - 1. The DACS shall support up to 32 door control modules to control 32 doors. Each door controller shall be capable of being programmed through the DACS from the local programmer or the RPS.

\*\* NOTE TO SPECIFIER \*\* B8512G. Delete if not required.

* + - 1. The DACS shall support up to 8 D9210C door control modules to control 8 doors.
      2. The DACS shall use 26 bits or 37 bits of card/token specific data to identify the user. The card data shall not be truncated or shortened in making the identification of the user.
      3. The access control module shall be able to be configured independently from the other doors. Door controllers shall include the following features and functions:
         1. Supervised, wired connection to normally open or normally closed contacts.
         2. 14 programmable levels of access authority
         3. Programmable entry/exit door strike and shunt control. The door opening can terminate a programmable door buzzer. The door contact is shunted when valid access is being granted through the door.
         4. A request to exit and a separate request to enter supervised input. A programmable feature provides for door shunting on request to exit without activating the lock output.
         5. Buzzer output that can be programmed to activate if the door is held open beyond a programmable time. Additionally, the ACC can display a door closing warning.
         6. The door can be programmed to activate an alarm or trouble in the door left open condition. The DACS shall be capable of transmitting the Door Left Open indication to the DACR.
         7. The door strike shall be capable of being programmed to automatically unlock if the area is completely disarmed and will not automatically unlock if the area is selectively disarmed.
      4. The DACS shall be capable of being programmed, on a time basis, to record access granted and or access denied events by door.
      5. The DACS shall allow each authority profile to specify whether users holding that authority are to be granted access into the area based on whether the area is completely disarmed, perimeter armed or completely armed.
      6. The DACS shall be able to automatically disarm the area or convert the arm state of the area from fully armed to perimeter armed based on the authority level assigned to the user and area or arm an area from a particular reader.
      7. Assigned users shall be able to manually control the door from an ACC by setting the door to Normal Operation, Manually Locked or Secured (valid cards will not operate).
      8. The DACS shall log access control events and accommodate programming capability for transmission of the events to primary and/or secondary DACRs, including door and user identity.
    1. Communication: The DACS shall be capable of reporting system events and supervisory reports including alarm, trouble, missing modules, restorals, system status, AC failure, battery status to primary and secondary off-site DACR’s. The following features shall be supported.
       1. The DACS shall be capable of communicating via dial-up analog telephone lines, over a LAN/WAN/Internet using a wired network interface module, or over a cellular network using a CDMA Cellular interface module.
       2. The Bosch Modem4 communications format shall be utilized for optimum system performance. The Modem4 format provides the maximum data information to the receiver for alarms, troubles, restorals, bypasses, relay activation, opening/closings, and card access. The detailed information includes the point numbers with text, peripheral device numbers, user numbers with text, and area information. As an alternative format, SIA DC09 or Contact ID may be used although they will include less detailed information like point or user text.
       3. The DACS shall be capable of sending text (SMS) messages to compatible devices without requiring that these message are sent to a monitoring center
       4. The DACS shall have the capability of communicating with up to 8 different DACRs using up to 4 different phone numbers, up to 24-digits in length and/or 4 URL/IP addresses over a network.
       5. The DACS shall report to a Commercial Central Station that is using a Bosch D6600 Receiver/Gateway or a Bosch D6100i Receiver using Modem4 as a preferred format or Contact ID as an alternate format.
       6. The DACR shall provide the transmission information sent from the DACS that includes alarms, troubles, restorals, bypasses, relay activation, opening/closings, and card access. When using the ModemIIIa² format the detailed information includes the point numbers with text, peripheral device numbers, user numbers with text, and area information.
       7. The DACS reports shall be classified, by event, into eleven subcategories or "report groups." Each group represents similar types of events. Individual events within each group shall be selectively enabled or disabled for transmission. The eleven report groups shall be as follows:
          1. Fire Reports.
          2. Burglar Reports.
          3. User Reports.
          4. Test Reports.
          5. Diagnostic Reports.
          6. Relay Reports.
          7. Auto Function Reports.
          8. RPS Reports.
          9. Point Reports.
          10. User Change Reports.
          11. Access Reports.
       8. The DACS shall have the capability to verify the integrity of the remote communications path and switch to alternate paths when a communications failure occurs.
       9. The DACS shall be capable of unattended mode of operation whereby programming and configuration updates are automatically transferred using the Remote Programming Software (RPS). These updates can initiate from either the control panel or the remote computer using RPS.
    2. Network Communication: The DACS shall be capable of network communications over a LAN, WAN, Intranet, or the Internet. The system shall include supervision of the network communication utilizing configurable periodic heartbeats to the Digital Alarm Communications Receiver (DACR). The DACR shall provide notification of the loss of communications from a networked system after a programmable timeframe since the last communication. The notification options shall be programmable and include local annunciation or indication to automation software.
       1. The network interface module shall be capable of supporting Dynamic Host Communication Protocol (DHCP) to obtain an IP Address.
       2. The system shall support a method of authentication between the control panel and the receiver to ensure that the control panel has not been compromised or replaced.
       3. The network interface modules shall be capable of supporting encryption using a minimum of 256-bit AES Encryption (Rijndael) certified by NIST (National Institute of Standards and Technology) utilizing the Cipher Block Chaining (CBC) method.
       4. The network interface module shall support a 10/100BaseT connection to an Ethernet network.
       5. The control panel shall be capable of network communication with a programmable poll time to send periodic heartbeats to the receiver, programmable ACK Wait time, and programmable retry time. In the situation where a communication path is unsuccessful, the control panel shall be capable of attempting backup communication through an available communication method to the same receiver or a backup receiver.
          1. The control panel shall have the ability to automatically adjust the heartbeat rate of a backup path that is using cellular to the heartbeat rate of the primary path in case of a primary path failure. Upon restoral of the primary path, the heartbeat rate of the backup path shall automatically restore to the original rate. This allows a system utilizing cellular communications to keep the wireless charges low.
          2. The network communication between the control panel and the receiver shall use Modem4, SIA DC09 or Contact ID.
          3. The control panel shall be capable of two-way communication using a wired network interface module with a 10/100BaseT on a LAN/WAN/Internet configuration or with a cellular module on the Internet.
          4. The control panel shall be capable of configuring the destination of the receiver using a URL or static IP Address.
          5. The control panel shall be capable of using DNS to lookup the IP Address of the receiver when programmed with a URL.
          6. The control panel shall support UPnP for automated Port Forward configuration in the router where the control panel is installed.
          7. The control panel shall support AutoIP to enable the RPS software to connect to the control panel locally using an IP Direct connection.
          8. The control panel shall support configuration of the IP parameters from the keypad eliminating the need for a PC to configure the IP device.
          9. The control panel shall support network diagnostics from a keypad to allow local testing of network connectivity. The diagnostics should include, Ethernet cable connected, gateway configuration ok, DNS lookup operational, and external network connectivity (such as the Internet) operational.
          10. The system shall be capable of meeting DCID 6/9 and UL 2050 standards.
    3. Event Log: The DACS shall maintain a log of events indicating time, day, month, year type of event, account number, area number, user ID, point text, user text and primary/secondary event route. The system shall allow the following characteristics:
       1. The DACS shall be capable of storing up to 10,000 events

\*\* NOTE TO SPECIFIER \*\* Delete if not required.

* + - 1. The DACS shall support viewing of logs locally at the ACC and remotely via an upload to a remote central station computer running the RPS software.
      2. The DACS shall provide notification via a report to the DACR when the event log reaches a programmable “percent full capacity". This allows retrieval of stored events via RPS to prevent any loss of event history.
      3. Group, signal type and area can route events to specific receivers.
      4. Each DACR shall be designated as a primary, backup, or duplicate destination for each report group. Assigning an event to multiple routing groups provides for duplicate destinations for the event. The transmission of grouped events allows the reporting of different types of information to different remote DACRs.
    1. Testing, Diagnostic, and Programming Facilities: The DACS shall be capable of sending (manually or automatically) test and status reports to remote DACRs.
       1. The DACS shall be capable of sending automatic tests daily, weekly or once every 28 days. Automatic test times shall be programmable to provide an offset of up to 24 hours from the current time.
       2. Automatic test reports shall be programmable to be deferred by one test interval if any other report is transmitted in the current interval.
       3. Automatic test reports and remote system access for diagnostics shall be supported via a remote central station computer with Remote Programming Software (RPS).
       4. The DACS shall be programmable locally or remotely. Programming shall be accomplished via a Keypad or a computer with a remote programmer and diagnostic software package (RPS).
       5. The DACS shall allow an on-site user to initiate remote programming while on-line with the servicing location. The remote programming device must provide a compare feature and allow for downloading either the stored program or the (un)modified program copied from the panel.
       6. The DACS shall allow the local programming option to be disabled and must provide a method to program a panel while no one is on premises, when the panel shares a line with an answering machine.
       7. The DACS shall accommodate IP Diagnostic to verify settings and operation of the network interface modules; Host name, MAC address, IPV4 address assignment. The IP Connection test shall include; Link test to verify physical cable integrity, Ping test to verify gateway response, ping test to verify address on the internet.
       8. Wireless point diagnostics shall include signal strength and device states of registered wireless points in the system.
       9. The number of system testing and programming sessions shall be restricted via the use of program locking features and passwords. Passcode protection in excess of sixteen million combinations is required.
       10. New modules support enhanced diagnostics through RPS
    2. Miscellaneous Features: Programmable alarm output timer, 4 programmable entry delay times, exit delay programmable by area, individually programmable point of protection text, point bypassing, key switch arming capability with LED outputs, and fire verification.

\*\* NOTE TO SPECIFIER Delete if not required.

* + 1. False Alarm Reduction: The DACS shall comply with all ANSI SIA CP-01 2010 requirements for false alarm reduction

\*\* NOTE TO SPECIFIER \*\* Delete if not required.

* + 1. Ambush Detection: The DACS shall include an early ambush feature that requires that the user disarm, and then inspect the facility within a specified time period, before entering their passcode or a different authorized passcode again. If the user does not enter a passcode a second time, a duress event is generated. If the user does enter a passcode within the specified time period, the system disarms.

\*\* NOTE TO SPECIFIER Delete if not required.

* + 1. Two man rule: The DACS shall include a programmable feature that requires 2 separate passcodes to be entered to disarm the system. After 1 passcode is entered, the system will prompt for a second passcode to be entered on the same ACC. Without the second passcode, the system shall not disarm.
    2. Dual Authentication: The DACS shall support Dual Authentication by area. Areas programmed for Dual Authentication require activate of a card and a passcode to allow access to system functions, arm/disarm, or access control doors.
    3. Area Re-Arm: The System shall support programmable area re-arm time of 1 minute to 24 hour.
    4. User-Programmable Features: The DACS shall provide a menu driven interface to provide a user-friendly command structure for programming / customizing the system to the operational criteria of the application. The DACS shall be capable of being operated via:
       1. The Command Structure.
       2. Menu / Command List.
  1. SYSTEM INTERFACE REQUIREMENTS
     1. Grounding: The Contractor shall properly earth ground the DACS to prevent electrostatic charges and other transient electrical surges from damaging the DACS panel.
     2. Primary power: The Contractor shall provide a dedicated 120 VAC power circuit to the DACS system. This circuit shall be connected to the emergency power system. The 120 VAC is stepped down to power the DACS panel using a class two, plug-in transformer. This power circuit shall be properly rated to continuously power all points and functions indefinitely in full alarm condition.
     3. Primary power supervision: When the primary power source fails, the system can be configured to report an "AC Fail" message to a commercial central station.
        1. The message can also be programmed to "tag-along" with another message transmitted to the central station.
        2. The system will always display a loss of primary power on the ACC and may be configured to provide additional audible warning.

\*\* NOTE TO SPECIFIER Delete if not required.

* + - 1. The transmission delay of this message is programmable from 5 seconds to 86 minutes with an optional 6 to 12 hour transmission delay
    1. Secondary power (standby battery): The Contractor shall provide adequate battery power as defined by the relevant application criteria, (UL 864 and UL 985 for alarm installations or NFPA 72 chapters for fire applications). Appropriate battery chargers shall be provided consistent with the battery back-up capacity. The most current accepted version of NFPA 72 and any applicable local codes or AHJ requirements must be met accordingly.
    2. Secondary power supervision: When the secondary power source experiences a 85 percent depletion of its standby capacity, the system can be configured to report a "Low Battery" message to a commercial central station. The system will always display a low battery condition on the ACC and may be configured to provide additional audible warning.
    3. Telephone interface: The control panel in the DACS shall be equipped with an optional phone line monitor and shall interface with the phone lines via RJ-31X jacks for supervision of the telephone line connection.
       1. The telephone line interface shall conform with FCC rules (Title 47 C.F.R. part 68).

\*\* NOTE TO SPECIFIER \*\* Delete if not required.

* + - 1. When a telephone line is determined to be out of service by the DACS panel, the event will be annunciated locally on the ACC and transmitted to the central station over the alternate communications interface. The transmission delay of this message is programmable from ten to two-hundred forty seconds.
    1. Ethernet Interface: The DACS shall include a integrated Ethernet interface module as the primary, or back-up means of communicating to a DACR.
       1. Built-in IP-based alarm transport, programming, and control
       2. The module shall accommodate 128 and 256-bit AES encryption using CBC (Cipher Block Chaining) mode.
       3. 10BASE T or 100BASE T network connection
       4. Full-duplex and half-duplex support

\*\* NOTE TO SPECIFIER \*\* Delete if not required.

* + 1. Cellular interface: The DACS may use a cellular radio module as the primary, or backup, means of communicating to a DACR. Up to 4 IP Addresses shall be available for routing system events. The supervision time shall be programmable with a range of 5 to 65,535 seconds. The module shall accommodate 128 and 256-bit AES encryption using CBC (Cipher Block Chaining) mode.
    2. Auxiliary function control interfaces: The DACS shall accommodate auxiliary functions such as activating bells, strobes, or lights and shall be accomplished using the optional application specific relay modules. These auxiliary interfaces shall be electrically isolated to avoid inter-system interferences or damage to the system.
    3. Wiring: The contractor shall provide cables consistent with the manufacturer's recommendations. The following general guidelines shall be followed for wiring installation:
       1. Wiring shall be appropriately color-coded with permanent wire markers. Copper conductors shall be used.
       2. All signal cables provided under this contract shall be Class II, plenum-rated cable where required. Where subject to mechanical damage, wiring shall be enclosed in metal conduits or surface metallic raceway.
       3. Data wires shall not be enclosed in conduit or raceways containing AC power wires.
       4. Where EMI may interfere with the proper operation of the DACS circuits, twisted/shielded cable shall be used.
    4. Environmental Conditions: The DACS shall be designed to meet the following environmental conditions:
       1. The system shall be designed for a storage temperature of -10° C to 70°C (14° F to 158°F).
       2. The system shall be designed for an operating temperature of 0° C to 50°C (32° F to 120°F).
       3. The system shall be designed for normal operation in an 85% relative humidity environment.
       4. The system shall meet or exceed the requirements of FCC rules Title 47 C.F.R. Part 15, Class B devices, and Part 68, IEC EMC directive
  1. ACCESSORIES
     1. System Accessories::

\*\* NOTE TO SPECIFIER \*\* Fill in blanks and duplicate lines below as applicable. List types and quantities (if appropriate for the type of project) of accessories required for the application. Refer to Intrusion Binder MSRP Price List for a full range of accessories in the following categories. Delete if not required.

* + - 1. Intrusion System Accessory: Model \_\_\_\_\_\_\_\_\_.
      2. Fire System Accessory: Model \_\_\_\_\_\_\_\_\_.

1. EXECUTION
   1. EXAMINATION
      1. Examine areas to receive devices and notify adverse conditions affecting installation or subsequent operation.
      2. Do not begin installation until unacceptable conditions are corrected.
      3. If preparation is the responsibility of another installer, notify architect of unsatisfactory preparation before proceeding.
      4. Ensure selected location is secure and offers protection from accidental damage.
      5. Location shall provide reasonable temperature and humidity conditions, free from sources of electrical and electromagnetic interference.
      6. Ensure power source is protected against accidental shutoff.
      7. Install all equipment and materials in accordance with the "current" recommendations of the manufacturer. The work shall also be in accordance with:
         1. Installation criteria defined in these specifications and in the construction documents.
         2. Factory Representative can be the Bosch Security Systems Inc Security Dealer.
         3. Approved submittals.
         4. Applicable requirements of referenced standards.
      8. The contractor shall provide the following services as part of the contract:
         1. Supervision of sub-contractors.
         2. Coordination of other contractors for system-related work (electrical contractor, finish hardware contractor, architect, and general contractor).
         3. Attending site construction/coordination meetings.
         4. Keeping updated construction drawings at the construction site.
         5. Meeting construction deadlines per the construction schedule.
      9. Programming of the system shall include the following tasks:
         1. Programming system configuration parameters (hardware and software, zone/circuit numbers, communication parameters).
         2. Programming operational parameters such as opening/closing reports and windows, system response text (custom English) displays of events, activation of relays that drive auxiliary devices, and identifying types of zones/loops.
         3. Programming passcodes according to the authorities and functions defined by the owner.
         4. Other system programming tasks required by the owner. These additional programming requirements shall be coordinated between the owner and the contractor.
         5. Operational Testing: The contractor shall perform thorough operational testing and verify that all system components are fully operational.
         6. Hard-copy System Printout: The contractor shall submit a hard-copy system printout of all components tested and certify 100 percent operation indicating all devices/panels/units have passed the test criteria set forth by the manufacturer.
         7. Acceptance Test Plan Form: An acceptance test plan form shall be prepared/provided by the contractor prior to the acceptance walk-through.
         8. This form shall include separate sections for each device/panel/unit as well as a column indicating the manufacturer's performance allowance/margin, a column indicating the result of the testing performed by the contractor (pass/fail), and an empty column for recording findings during the walk-through.
         9. Fire Alarm Systems shall comply with NFPA 72 Standards for inspection, testing, and maintenance.
      10. The contractor shall certify completion in writing and schedule the commissioning walk-through. The contractor shall provide all the tools and personnel needed to conduct an efficient commissioning process.
   2. FIELD QUALITY CONTROL
      1. Installation contractor shall submit a written test report that the system has been 100 percent tested and approved. Final test shall be witnessed by the owner, engineer, electrical contractor, chief security officer, and performed by the installation contractor. Final test report shall be received and acknowledged by the owner prior to request for final payment.
      2. Provide instruction to the owner's satisfaction with regard to proper use and operation of the system.
      3. Determine and report all problems to the manufacturer's customer service department.
   3. ADJUSTING
      1. System maintenance and repair of system or workmanship defects during the warranty period shall be provided by the Contractor free of charge (parts and labor).
      2. Periodic testing of the system shall be carried out on a monthly or quarterly basis to ensure the integrity of the control panel, the sensing devices, and the telephone lines.
      3. The installer shall correct any system defect within six hours of receipt of call from the Owner.
   4. DEMONSTRATION
      1. Demonstrate at final inspection that surveillance system and devices functions properly.
         1. The Contractor upon completion of installation shall furnish training in the complete operation of the systems.
   5. PROTECTION
      1. Protect installed products until completion of project.
      2. Touch-up, repair or replace damaged products before substantial completion.

END OF SECTION