EIGHTH ARMY REGULATION 190-15

MILITARY POLICE (190)

Joint-Services Interior Intrusion Detection System (J-SIDS)

1 March 2010

UNCLASSIFIED

DEPARTMENT OF THE ARMY
HEADQUARTERS, EIGHTH UNITED STATES ARMY
APO SAN FRANCISCO 96301

REGULATION
NUMBER 190-15

AGJ LIBRARY
REFERENCE SET

1 March 2010

Military Police

JOINT-SERVICES INTERIOR INTRUSION DETECTION SYSTEM (J-SIIDS)

Supplementation by major subordinate commands is not authorized without prior approval by the Office of the Provost Marshal, HQ, USFK/EUSA. This does not preclude extracting information from this regulation to be used in local standing operating procedures (SOPs).

1. PURPOSE. To assign responsibilities and establish procedures for the acquisition, installation, maintenance, training of personnel, and operation of J-SIIDS within Eighth United States Army (EUSA).

2. SCOPE. This regulation is applicable to all units, organizations, activities and agencies assigned/attached to or under the jurisdiction of EUSA. This regulation delineates responsibilities for the staff and subordinate commands and activities to effect the management and proper use of J-SIIDS within EUSA.

3. GENERAL. a. The installation of J-SIIDS in arms storage facilities within EUSA will be considered by commanders immediately subordinate to this headquarters on a case by case basis to replace other means of continual surveillance recognized by DOD Manual 5100.76-M and AR 190-11. Consideration will include a comparison of the security provided by present surveillance and J-SIIDS and a cost comparison of the methods. Consideration must also be given to projected construction and deployment plans.

b. Consideration, as defined in paragraph 3(a) above will be the same for all other facilities which contain sensitive or high-value items prior to programming the installation of J-SIIDS.

4. RESPONSIBILITIES. a. The Provost Marshal, EUSA is the principal staff officer for J-SIIDS actions within this command. As such, the Provost Marshal will:

(1) Provide technical staff supervision for the security aspects of the overall J-SIIDS program to include:

(a) Monitoring the establishment and training of the response forces.

(b) Monitoring training for user personnel.

(c) Evaluating standard operating procedures developed by response forces and user units/activities.

(d) Insuring that adequate coordination is maintained between local Provost Marshals and Area Facilities Engineers (AFE) to resolve J-SIIDS problems in a timely manner.

(2) Act as the reviewing authority for J-SIIDS installation/removal requests submitted by installation and area commanders.

b. The Commander Facility Engineer Activity-Korea (FEA-K) is the responsible staff officer for J-SIIDS procurement, installation, and maintenance actions within the command. As such, FEA-K will:

(1) Coordinate and process off-line procurement/requisitions submitted by local AFE.

(2) Establish procedures for and supervise maintenance operations to include:

(a) Managing repair and spare parts.

(b) Providing periodic technical training of AFE personnel to insure that a technically proficient labor pool is available to install and repair J-SIIDS systems.

(c) Coordinating with ACofS, J-6 for installation and maintenance of telephone cable transmission lines.

(d) Appointing a J-SIIDS program manager at each AFE.

(3) Coordinating with the Troop Support & Aviation Readiness Command field maintenance technician for technical guidance and assistance.

(4) Monitoring J-SIIDS operational status and insuring that required reports are submitted as appropriate with an information copy to Cdr, EUSA, ATTN: PMJ-S, APO 96301.

(5) Evaluating the operation of installed systems and supervising retrofit and upgrade requirements to insure effective operation of J-SIIDS at the user level.

(6) Establishing a periodic maintenance evaluation schedule for installed systems as an active maintenance management program.

c. ACofS, J-6 will:

(1) Supervise maintenance and upgrade of telephone cable transmission lines in support of J-SIIDS.

(2) Supervise installation/dedication of telephone cable transmission lines required for J-SIIDS.

(3) Program and budget for cable requirements for J-SIIDS.

d. Installation and area commanders will:

(1) Develop a precedence listing of facilities requiring J-SIIDS which includes justification and cost data within their area or installation in conjunction with the local supporting provost marshal, AFE, and area signal officer.

(2) Submit requests for installation of J-SIIDS through the local provost marshal to the Commander, EUSA, ATTN: PMJ-S, APO 96301, for technical approval.

(3) Develop procedures to respond to alarms in accordance with (IAW) the following guidance.

(a) A Response Force Team (RFT) armed with individually assigned weapons or shotguns will be organized by the monitor area supervisor to respond to any activation of the intrusion detection alarm. Organization of the response force will consist of a minimum of two guards. The senior member will be designated the team leader.

(b) Upon activation of an alarm, the RFT will be immediately dispatched to the location of the facility being monitored. One guard will go forward and make a visual check of all entrances to the facility to ascertain if a penetration attempt has been made. The other guards will take up a secure position taking maximum advantage of available cover and will keep the guard who is conducting a visual check of the entrances in sight at all times, thereby providing security in the event that armed resistance is encountered. In the event that evidence of penetration, attempted penetration or tampering is discovered, the team leader will immediately call the Military Police Station and inform them of the building/room location and that an attempted break-in has occurred. The team leader will insure that guard personnel detain any persons attempting to leave the vicinity, pending arrival of Military Police. The team leader will accompany the Military Police into the facility to check for the presence of intruders.

(c) For arms or ammunition storage facilities, the responsible commander will immediately dispatch responsible individuals to conduct a visual count/inventory of the storage facility. Care must be taken while conducting the inventory not to touch or disturb anything which might have any value as evidence. If any losses are discovered, the area will be sealed as a crime scene pending arrival of investigative personnel. After completion of the investigation, the team leader will secure the building and insure the alarm is reset. If the structure cannot be secured adequately or if the alarm does not function, the responsible commander will post a guard at the entrance of the facility until repair can be accomplished.

(d) After completing the visual inspection and no evidence of a penetration or attempted penetration is discovered, one or more guards will remain at the scene. One guard will go to the nearest telephone to notify the monitor operator that all is secure and will subsequently inform the monitoring operator when entrance is made into the facility to reset the monitor module status. The security force will return to the monitor/guard location.

(e) Response forces will be required to respond to the location of a protected facility within five minutes after receipt of an alarm signal from the facility.

(f) Periodic tests, at least monthly, will be performed requiring the response force to respond to simulated alarms and to insure personnel are familiar with procedures and that their response is within the time frame established in paragraph (e) above.

(g) Whenever a monitor location contains monitor panels from different units/activities, the commander of each protected unit/activity will provide personnel for the response force. Respective commanders will coordinate a written agreement delineating individual responsibilities in support of response force. This agreement will be updated annually or upon reassignment, transfer, or other permanent loss of any signatory to the agreement.

(h) The person having custody of the protected area keys will be capable of responding to the protected area within 10 minutes after notification of an alarm.

(4) Determine the location(s) of J-SIIDS monitoring unit(s), taking into consideration that personnel must be available to monitor and respond to all alarms. The response requirement may be met by other than military police resources.

(5) Require unit commanders/activity chiefs utilizing J-SIIDS to submit requests for maintenance and repair directly to the servicing AFE.

e. Area/installation provost marshals will:

(1) Establish detailed guidance for military police response to the scene of a protected area which has experienced an actual or attempted intrusion/break-in. The requirements for military police response are outlined in para 4d(3)(b) of this regulation.

(2) Maintain close liaison with the AFE J-SIIDS program manager.

(3) Provide technical assistance concerning operation and testing procedures to user activities as requested.

f. Unit commanders/activity chiefs will insure that:

(1) All personnel responsible for the operation of the control unit are properly trained.

(2) The procedures outlined in Appendix A, this regulation, as they pertain to operation and maintenance of the control unit and sensors, are complied with.

(3) Tests of the system are conducted at least once every two weeks as outlined in Appendix B.

(4) Malfunctions in the system are reported to the monitor station and the AFE work order reception desk immediately after discovery. If not repaired within 24 hours of initial report, notification will be made to the Commander, AFE, and local Provost Marshal Office (PMO).

(5) When a system protecting facilities which store documents, arms, or ammunition malfunctions, the facility is placed under continuous surveillance until the system is repaired and operational.

(6) All administrative records required by paragraph 6 of this regulation are maintained for a period of 180 days.

(7) Requisitions for J-SIIDS are prepared and forwarded to local AFE.

(8) J-SIIDS requirements are adequately budgeted and funded.

(9) A supervisor of the monitored area is appointed. Commanders/activity chiefs of organizations served by a J-SIIDS will appoint a supervisor of the monitored area, usually the physical security officer or S-2, as the individual exercising overall supervision of the J-SIIDS program in the organization. In those instances where more than one organization is served by a monitor station, the higher organization will appoint a supervisor of the monitored area who will exercise overall supervision of all J-SIIDS systems serviced by the monitor station.

(10) Insure that the supervisor of the monitored area:

(a) Establishes and maintains close coordination and liaison with supported commanders.

(b) Establishes written SOPs to include response force deployment and provisions for tasking of supported units to provide personnel necessary for staffing a response force on a prorata basis based on the number of protected facilities within each unit.

(c) Insures that personnel utilized as monitor operators are thoroughly briefed on their responsibilities and understand the operation of the monitor cabinet before assuming duty. Detailed instructions for the operation of monitor cabinets are contained in Appendix C.

(d) Develops and distributes a (duress) identification code for use by control unit operators and monitor operators. Instructions for using the duress identification code are in Appendix D.

g. Monitor operators will:

(1) Maintain constant surveillance of the monitor cabinet during their tour of duty.

(2) Maintain all administrative records required by paragraph 6 of this regulation.

(3) Immediately report malfunctions in the J-SIIDS to the AFE work order reception desk, and record the information on AA Form 212-R (Appendix E).

(4) Immediately notify the response force team leader of any alarm. This notification will include:

(a) Exact location of the building (e.g., building number and street location where the alarm occurred).

(b) What type alarm has been experienced (if possible).

(5) Verify the identity of each control unit operator by use of the current identification code.

h. AFE will:

(1) Appoint and maintain a qualified individual as the J-SIIDS program manager. The individual will be trained in and fully knowledgeable of J-SIIDS maintenance and installation procedures.

(2) Install and maintain all J-SIIDS systems and jointly conduct an acceptance inspection of any new installation with a representative from the supporting PMO, Physical Security Section.

(3) Provide the local provost marshal, ATTN: Physical Security Section, with a roster of all personnel authorized to perform maintenance on J-SIIDS systems.

(4) Conduct a monthly maintenance inspection to insure systems are operating properly.

(5) No later than the last working day of each month, provide the local Provost Marshal Physical Security Section a written status report of all J-SIIDS to include:

(a) Number of installed systems by category (e.g., arms, ammo, other).

(b) Number of operational systems by category.

(c) Number of inoperative systems and reason(s) for inoperative status/failure (to include total time down).

(d) Status of supply actions concerning requisitions of replacement parts/components, etc.

i. Commander, 1st Signal Brigade will provide support as required for the installation and maintenance of transmission lines for alarm transmission.

5. KEY CONTROL. a. J-SIIDS keys will be maintained separate from other keys and will be accessible only to those individuals whose official duties require access to them. A current roster of these individuals will be kept within the unit, agency, or organization and will be marked For Official Use Only (FOUO).

b. EA Form 218 (Key Control Register) will be maintained at all times to insure administrative accountability for keys.

c. At no time will keys be left unattended or unsecured.

d. Reproduction of keys at unit/activity level is not authorized.

e. In the event of lost or stolen keys, affected locks will be replaced immediately. Should keys be lost, misplaced, or stolen, the local provost marshal will be notified immediately.

f. After duty hours, keys will be secured in a locked container constructed of at least 20-gauge steel or material of an equivalent strength or in the custody of a responsible duty officer or noncommissioned officer.

g. A key and lock custodian will be appointed to insure the proper custody and handling of keys.

h. All keys to J-SIIDS will be under the control of the commander of the protected area or a designated representative.

i. When one monitor is established for several protected area facilities, the monitor activity commander will establish control and accountability of both monitor unit keys.

j. The reserve/back-up set of keys to the control unit will be secured separately from the operational set of keys.

k. J-SIIDS key registers will be maintained for 180 days, then destroyed.

l. J-SIIDS keys will be inventoried monthly and recorded on DA Form 2496 (Disposition Form).

6. FORMS AND RECORDS. a. Each time a status change is indicated on the Status Monitor Module the information will be recorded on EA Form 212-R (J-SIIDS Opening/Securing Alarm Record) shown at Appendix E to this regulation. Entries will include the following:

(1) Building number and description (i.e., arms room, post exchange, etc.).

(2) Unit/facility protected.

(3) Who opened the facility.

(4) Who secured the facility.

(5) Time opened.

(6) Time closed.

(7) Status changes.

(8) Cause of alarms.

(9) Reaction force arrival times.

(10) Tests conducted.

(11) Engineer notifications pertaining to system malfunctions.

(12) Other information as required.

b. EA Form 212-R will be retained on file at the monitor station for a period of 180 days.

7. TRAINING. a. Training will be conducted by local provost marshals.

b. The following categories of personnel will attend provost marshal training classes for instruction in the operation of J-SIIDS.

(1) Operators of the control unit portion of the J-SIIDS.

(2) Key personnel performing the duties of monitor operator.

(3) Personnel who exercise direct control over the operation of facilities in which J-SIIDS are installed and those who exercise supervision over response forces.

c. Requests for school quotas/scheduling will be forwarded through command channels to the local provost marshal.

d. Personnel operating any component of the J-SIIDS must have received training on the correct operation of the system.

8. MAINTENANCE/INSTALLATION. a. It is prohibited to place any object(s) on or near the control unit, monitor cabinet, or other component part of the J-SIIDS.

b. Operators will keep the exterior of all J-SIIDS components clean, free of dust, dirt, trash, or other debris.

c. The outer surface of J-SIIDS components will be cleaned daily with a clean, dry cloth. Sprays, cleaning fluids, or liquids of any type will not be used to clean cabinets.

d. Care will be taken when cleaning J-SIIDS components not to dislodge, break, or otherwise cause damage to switches, lights, or other equipment. Special attention must be taken when using a broom or mop around the alarm latching switch (duress alarm) to prevent accidental activation of the switch located in the front of the sensor. Water or other liquids will be kept clear of the floor area immediately surrounding the alarm latching switch.

e. Caution/warning labels affixed to J-SIIDS cabinets will not be removed, defaced, mutilated, or otherwise damaged. Damaged/missing labels will be reported promptly to AFE.

f. J-SIIDS will be installed by qualified engineer personnel only.

g. Rosters indicating persons authorized to open/secure the protected area and perform maintenance on J-SIIDS will be provided as indicated below:

(1) A roster (indicating name, SSN, and telephone number) at the protected area and provided to the monitor station. Any changes will necessitate publication of a new roster. A roster will be maintained in a location where it is readily available to the monitor cabinet operator.

(2) A roster (indicating name, SSN, and telephone number) of authorized J-SIIDS maintenance installer personnel will be provided to the monitor unit location and to the protected area. Only those personnel who have had favorable checks completed as outlined in subparagraph (3), below, will be included on this roster.

(3) Prior to having access to J-SIIDS, all US installers/maintainers of J-SIIDS and operators of monitor cabinets/modules must have, as a minimum, a favorable National Agency Check and Entrance National Agency Check.

Local nationals must have a favorable Korean National Agency Check supplemented by a local file check with the area provost marshal or any other agency that might have information on file which would reflect on the honesty or stability of the individual.

h. Maintenance of J-SIIDS components will be performed only by qualified engineer maintenance installer personnel.

i. There are no authorized modifications for the switch alarm latching (foot activated duress switch). The switch alarm latch cover will not be modified in such a manner as to reset the alarm without removing the cover.

j. A system installation wiring diagram, along with grid wire dimensional diagram (when grid wire sensors are installed), will be drawn up for each protected area. The diagram will indicate which sensors are installed and show color coded interconnections between each sensor and the unit. All systems options (alarm option, length of time delays, type of monitor module system reports to, signal transmission option) should be indicated on the diagram. The diagram will be maintained by local engineers and must be stored inside the control unit door in the space provided. Such documents will be marked "For Official Use Only."

k. The telephone number at the monitor cabinet location will be provided to the protected area and will be recorded on the control unit operating procedures cards.

9. INSPECTION. a. Installation physical security inspectors will include a check of each intrusion detection systems (IDS) during any announced or unannounced security inspection of a unit/activity. Checks will include visual inspection of components and conduit for evidence of tampering and operational checks of the system IAW procedures outlined in Appendix B and F. This same test can be modified and applied to any commercial system. Checks will also be made of log entries and records regarding operation and inspection of IDS. Results of IDS Inspections will be noted on DA Form 2806 (Physical Security Survey).

b. Prior to operational acceptance of a newly installed IDS system, an inspection will be conducted to insure the system meets the minimum acceptable standards. The inspection will be conducted IAW AR 190-13 by installation physical security inspectors and AFE representatives.

10. LOCATION OF J-SIIDS COMPONENTS. a. Sensors will be positioned within the protected area at locations that provide the best overall protection. Sensors will be utilized in sufficient quantities to insure that the entire area is protected without operating the sensors at maximum sensitivity.

b. Control units should be mounted on the interior wall of the protected facility as close as possible to the main entrance door.

c. Monitor units will be installed in such a location that the status display is not obstructed from the continual view of monitor personnel.

d. The alarm latching switch (duress alarm) should be positioned inside the protected area at a location where it is readily available to on-duty personnel and can be operated without obvious observation of an intruder.

e. Additional levels of protection, where practical, are encouraged. In selecting the mode of operation desired for each facility it must be understood that J-SIIDS is designed to detect, not prevent, an intrusion. Therefore, a comprehensive physical security plan must contain appropriate physical security measures along with procedures for an effective response force. To insure this, J-SIIDS will be installed in such a manner that alarm signals can only be cleared by entering the protected area. Remote clearing of alarms prior to entering and checking the facility is not authorized.

11. REFERENCES. a. AR 190-11 (Military Police-Physical Security of Weapons, Ammunition and Explosives).

b. AR 190-50 (Military Police-Physical Security for Storage of Controlled Medical Substances and other Medically Sensitive Items).

c. AR 190-51, Appendix G (Security of Army Property at Unit and Installation Level).

d. FM 19-30 (Physical Security).

e. TM 5-6350-262-14/14, Technical Manual Operator, Organizational, and Intermediate Direct Support and General Support Maintenance Manual Installation, Operation and Check-Procedures for Joint-Services Intrusion Detection System (J-SIIDS).

The proponent agency for this regulation is the Office of the Provost Marshal. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Cdr, EUSA, ATTN: PMJ-S, APO 96301.

FOR THE COMMANDER:

OFFICIAL:

JOSEPH T. PALASTRA, JR.
Major General, USA
Chief of Staff

Jesse C. Heredia
JESSE C. HEREDIA
CPT, AGC
Assistant Adjutant General

6 Appendixes
A. Control Unit Operating Procedure
B. Abbreviated System Checkout Procedure
C. Monitor Cabinet/Module Operating Procedure
D. Identification Code (Duress)
E. EA Form 212-R
F. Controls and Indicators

DISTRIBUTION:
A and J (J less AGJ-AP, PPCK)
200 - PMJ-S

CONTROL UNIT OPERATING PROCEDURES

1. Securing the protected area:

a. Insure that all personnel have left the protected area.

b. Shut all doors and windows in the protected area and secure them.

c. Inform personnel at the monitor station that you are preparing to secure the protected area. Give the applicable identification code to identify yourself. A card should be placed near the telephone with the telephone number of the monitor station recorded on it.

d. Verify that the control unit AC power indicator light is on.

e. Turn the control unit key operated mode switch to the SECURE mode.

f. Promptly remove the key, leave the protected area through the main entrance door, and secure the main entrance door(s).

g. Verify with personnel at the monitor station that a change from ACCESS to SECURE was received. If a change of mode was not received or if alarm is activated, re-enter the protected area, switch the control unit to ACCESS mode, and then repeat the above procedure. If after repeating the procedure, a SECURE status is still not shown at the monitor, report the deficiency immediately to the work reception desk, AFE. After duty hours, a guard must be placed at the protected facility until repairs have been completed and IDS functions properly.

2. Opening the protected area:

a. Inform the monitor station that you are about to enter the protected area.

b. Unlock the main entrance door(s), proceed directly and promptly to the control unit, insert the key in the mode control unit switch and turn to the ACCESS position.

c. Verify with the monitor station that an alarm was transmitted when the room was entered and that the system is now in the ACCESS mode.

3. EA Form 212-R will be maintained by control unit operators using the monitor record procedures in paragraph 6.

ABBREVIATED SYSTEM CHECKOUT PROCEDURES

The following procedure will be used at least once every two weeks to test the performance of the system.

1. Inform personnel at the monitor location that a system test is to be performed. Be certain to give the correct identification code (duress) to monitor operators to properly identify yourself.

2. Telephone contact will be maintained with the monitor operator to insure test alarms and status changes are displayed on the monitor module.

3. Before beginning the test insure all doors and windows are secured.

4. Turn control unit switch to test/reset position.

5. Ultrasonic motion sensor (UMS) check. (See page 1-32, Figure 1-23, TM 5-6350-262-14/14 for description.)

a. Proceed to area farthest away from UMS, position yourself facing it and stand motionless until the audible tone from the control unit ceases.

b. Take one short 24-inch step toward the UMS, then remain motionless. An audible tone from within the control unit should sound for 10 seconds, provided personnel stand motionless and do not activate another sensor.

c. Proceed to the next sensor type to be tested and stand motionless until the audible tone from the control unit ceases.

6. Balanced magnetic switch check. (See page 1-18, Figure 1-13, TM 5-6350-262-14/14 for description.)

a. Slowly open the door or window protected by the balanced magnetic switch. An audible tone from the control unit should sound.

b. Close the door or window and proceed to the next sensor type to be tested and stand motionless until the audible tone from the control unit ceases.

7. Passive ultrasonic sensor check. (See page 1-29, Figure 1-21, TM 5-6350-262-14/14 for description.)

a. Stand at various places in the protected area and lightly rattle keys on a key ring at short intervals. Rattles should be spaced a few seconds apart. An audible tone from the control unit should sound.

b. Proceed to the next sensor type to be tested and stand motionless until the audible tone from the control unit ceases.

8. Switch alarm latching (foot activated duress switch). (See page 1-38, Figure 1-28, TM 5-6350-262-14/14 for description.)

a. Activate the switch by placing the toe of shoe or boot under the shroud and lift gently. An audible tone in the control unit should sound.

b. Turn the control unit mode switch to ACCESS. The audible tone should cease.

c. Insure that the light on the duress switch is on.

d. Remove the cover of the housing by removal of the four screws at each corner.

e. Depress both reset buttons in the center of the unit.

f. Insure that the light on the front has gone out.

g. Replace the cover and the screws.

9. Refer to Chapter 5, Section V, TM 5-6350-262-14/14 for instructions on performing abbreviated tests on other types of sensors that are installed.

MONITOR CABINET/MODULE OPERATING PROCEDURES

When assuming responsibility for attending the monitor cabinet(s), insure that all alarm (red) lights are off, that all AC power lights (white) are on, and that the proper operating mode (ACCESS or SECURE) is indicated on all status monitor switches in the LAMP TEST position. If lights are burned out, report it to AFE work reception desk unit for repair.

1. Alarm indicator lights (red) flashing and an audible tone sounding:

a. Momentarily place RESET/ACK switch on the monitor module in the ACK position.

b. If the alarm is not generated during a scheduled or prearranged system test, direct the response force to respond to the protected area. NOTE: If an alarm occurs when the SECURE LIGHTS (green) are on, a high probability exists that an intrusion is in progress. If an alarm occurs when ACCESS lights (yellow) are on, high probability exists that personnel are tampering with the system in the protected area or that personnel in the protected area are in danger. The response force should be provided with this information if possible.

c. After the response force has investigated the cause of the alarm and responsible personnel have reset the control unit at the protected area, momentarily place the RESET/ACK switch in the RESET position to extinguish the alarm (red) lights.

2. Monitor AC power indicator lights (white) flashing and an audible tone sounding:

a. Momentarily place LAMP TEST/ACK switch on the monitor module in the ACKNOWLEDGE position.

b. If the lights extinguish, inform the local AFE work reception desk, that the AC power to the monitor cabinet has just failed. (The batteries will automatically take over for approximately 24 hours until AFE can restore AC power.)

c. If the lights continue to burn steadily, this is the normal condition.

3. ACCESS indicator lights (yellow) are flashing and an audible tone is sounding:

a. Momentarily place RESET/ACK switch on the monitor module in the ACK position.

b. If the change to ACCESS is not a prearranged or scheduled opening of the protected area, direct the response force to respond to the protected area.

4. SECURE indicator lights (green) are flashing and an audible tone is sounding:

a. Momentarily place the RESET/ACK switch on the status monitor module in the ACK position.

b. If the change to SECURE status is not part of a prearranged or scheduled securing of protected area, direct the response force to the protected area to insure that the area is physically secure.

5. AC power indicator lights (white) flashing and an audible tone is sounding:

a. Momentarily place RESET/ACK switch on the status monitor module in the ACK position.

b. If the lights extinguish, inform the AFE work reception desk that AC power to the protected area has just failed. NOTE: AC power failure at the protected area may be an indication of an attempted intrusion. The response force should be dispatched to the protected area to check for evidence of line tampering. The response force should be advised to proceed with caution. The battery within the control unit of the protected facility will take over automatically for up to 24 hours. If the battery goes dead prior to the AC power being restored, an alarm will automatically be transmitted and a guard must be posted at the protected facility.

c. If the AC power lights stay lighted steadily, this is a normal condition.

6. Panel monitor personnel performing monitor duty will be exempt from all duties except those necessary to monitor alarms. Panel monitor personnel, while in the performance of their duties, should not be allowed to engage in any activity, such as watching television, playing cards, reading, etc., which would distract their attention from the monitors.

IDENTIFICATION CODE (DURESS)

1. The monitor station commander will formulate and prepare an identification code (duress), preferrably some word or statement which can be used in normal conversation without arousing the suspicion of any would be perpetrators. However, the code should not be so common that an individual would routinely use the code in everyday conversations.

2. Codes will be disseminated to each unit armorer or protected facility operator, monitor operator, and response force member.

3. Codes will be used for proper identification by each individual reporting any information to the monitor operator.

4. Codes will be changed whenever a change is made in personnel assigned as armorer, protected facility operator, or monitor operator or at any time it is suspected that the code has been compromised.

5. Protected facility operators will be instructed that if they are placed under duress they will use the code when reporting to the monitor operator during opening or closing of the protected facility.

J-SIIDS OPENING/SECURING/ALARM RECORD
(EUSA Reg 190-15)

BLDG #

UNIT:

OPENING AND SECURING OF PROTECTED AREA					ALARMS		
DATE	OPENED BY	TIME	SECURED BY	TIME	TIME	REACT: FORCE ARR: TIME	CAUSE OF ALARM/STATUS CHANGE/REMARKS

EA FORM 212-R, 1 Mar 82 Replaces JK Form 212-R, 1 Oct 76, which is obsolete.

CONTROLS AND INDICATORS

1. Control unit. a. Mode switch (three position key operated switch, key removable only in the secure position). Selects the mode of system operation by:

(1) ACCESS: Inhibits intrusion alarms. When the key is in the access position, only the tamper and duress alarms will function. This position is used when authorized personnel are working in the area.

(2) SECURE: Reports tamper, duress, and intrusion alarms. Selected when the area is secured.

(3) TEST/RESET: Audibly indicates all intrusion, duress, and tamper alarms at the control unit alarm outputs and audible alarm. Selected when performing system tests or resetting the alarm.

b. AC power indicator light (white). An absence of light indicates failure of AC power to the control unit (provided bulb is not burned out).

2. Monitor cabinet and modules. a. Monitor AC power. Indicated by two white lights located on the monitor cabinet signal module. Reports the status of AC power as follows:

(1) Presence of continuous light from one or both indicator lights indicates AC power is being supplied to the monitor cabinet.

(2) Absence of light from both lights indicates AC power to the monitor cabinet has failed (provided bulbs are not burned out).

(3) Flashing of one or both lights indicates AC power has just failed or has just been restored to the monitor cabinet, depending upon condition of lights after LAMP TEST switch is momentarily placed in the ACKNOWLEDGE position.

b. LAMP TEST/ACKNOWLEDGE switch. Located on the monitor cabinet signal module. Performs tests or reset of the monitor panel AC power by:

(1) LAMP TEST position: Tests the monitor AC power indicator lights.

(2) ACK position: Resets the monitor AC power indicator lights from flashing state to steady state (on or off) depending on status of AC power to the monitor cabinets, and silences the audible alarm tone from the monitor cabinets.

c. AC power indicator lights. The two white lights located on each status module reports the status of AC power to the control unit by:

(1) Steady light from one or both indicator lights indicates AC power is being supplied to the protected area control unit.

(2) Absence of light from both indicator lights indicates AC power to the protected area control unit has failed (provided bulbs are not burned out).

(3) Flashing of the indicator lights indicates AC power to the protected area control unit has just failed or has just been restored, depending on steady state condition of lights after RESET ACK switch on status monitor module is momentarily placed in the ACK position.

d. ACCESS indicator lights. The two yellow lights located on the status monitor module indicate that the protected area control unit is in the ACCESS mode by:

(1) Steady light from one or both indicator lights indicates the protected area control is in the ACCESS mode of operation. When the ACCESS indicator lights are on, the SECURE indicator lights should be off. When the ACCESS indicator lights are off, the SECURE indicator lights should be on, provided both ACCESS indicator lights are not burned out.

(2) Flashing of the ACCESS indicator lights indicates that the protected area control unit has just been switched into the ACCESS mode of operation. Momentarily placing the RESET/ACK switch in this position will cause the SECURE indicators to extinguish and the ACCESS indicator lights to burn steady.

e. SECURE. Is indicated by the two green lights by:

(1) Steady light from one or both indicator lights indicates that the protected area control unit is in the SECURE mode of operation. When the SECURE indicator lights are on, the ACCESS indicator lights should be on provided both SECURE indicator light bulbs are not burned out.

(2) Flashing of the SECURE indicator lights indicates the protected area control unit has been switched into the SECURE mode of operation. Momentarily placing the RESET/ACK switch in the ACK position will cause the ACCESS indicator lights to extinguish and the SECURE indicator light to burn steady.

f. Alarm. Two red indicator lights indicate alarm status when lighted by:

(1) Absence of light indicates the normal condition (provided both bulbs are not burned out).

(2) Flashing of the red lights indicates an intrusion, duress, or tamper alarm has just been generated in the protected area. Momentarily placing the RESET/ACK switch in the ACK position will cause the buzzer to silence and the alarm lights to burn steady. If the alarm condition is due to telephone line noise of short duration, the alarm indicator lights can be extinguished by momentarily placing the RESET/ACK switch in the RESET position.

g. RESET/ACK switch. A two position spring loaded switch for silencing alarms and resetting the mode indicator lights by.

(1) ACK position: Silences the audible tone from the monitor cabinet signal module and causes flashing lights to burn steady.

(2) RESET position: Extinguishes the alarm indicator lights on the monitor module when alarm input to the monitor has ceased.

h. LAMP TEST. Switch located on the status monitor module and on the alarm monitor module will test all indicator lights on the modules when depressed.