BY ORDER OF THE COMMANDER
377TH WEAPONS SYSTEM SECURITY SQUADRON (WSSS)
KIRTLAND AIR FORCE BASE (AFGSC)

WSSS SOP 31-101, Volume 4
14 June 2016

Security Forces

KIRTLAND UNDERGROUND MUNITIONS MAINTENANCE & STORAGE COMPLEX (KUMMSC) AUTOMATED ENTRY CONTROL SYSTEM (AECS) OPERATIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is only available directly from the Office of Primary Responsibility (OPR).

RELEASABILITY: Access to this publication is restricted: this publication is classified Department of Defense (DoD) Unclassified Controlled Nuclear Information/For Official Use Only (DCNI/FOUO). This publication may not be released to foreign nationals; requests for accessibility must be approved by the OPR.

OPR: 377 WSSS/S3OS

Certified by: 377 WSSS/CC
(Lt Col James K. Meier)

Supersedes: WSSS SOP 31-101 Volume 4, 16 February 2016

[Pages: 66]

PURPOSE: This 377th Weapons System Security Squadron (WSSS) Standard Operating Procedure (SOP) implements AFMAN 31-108, *Air Force Nuclear Weapons Security Manual* and establishes guidance governing the authority, procedures, responsibilities, duties, standards, tasks and requirements for all WSSS operations. This instruction establishes procedures and requirements regarding Automated/Advanced Entry Control System (AECS) operation, Perimeter Surveillance Radar System (PSRS) Operation, X-ray Operation, and Metal Detector Operation. This publication does not apply to Air Force Reserve Command (AFRC) Units. This publication does not apply to Air National Guard (ANG). Refer recommended changes and questions about this publication to the Office of Primary Responsibility using AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm.** The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

Table of Contents

CHAPTER 1
AUTOMATED/ADVANCED ENTRY CONTROL SYSTEM (AECS)

1.1. (DCNI) Introduction. This chapter describes terminology and capabilities of equipment, and operator responsibilities associated with the Kirtland Underground Munitions Maintenance And Storage Complex (KUMMSC) Linx Predator Elite (LPE) AECS.

1.2. AECS Terminology.

1.2.1. Intrusion Detection System (IDS). A system designed to increase detection capability by alerting posted Security Forces (SF) to an approach, intrusion, or attempted intrusion. IDS provides in-depth detection and assessment capability through the use of detection and assessment devices.

1.2.2. Closed Circuit Television (CCTV). A system comprised of cameras and monitors that enables near real-time immediate visual assessment (IVA). The Burle CCTV network device enables AECS Automatic CCTV Call-Up and manual CCTV Call-Up functions, loss of communication to this device will disable these two functions. The CCTV video switcher system keyboard allows manual control over CCTV cameras and monitors.

1.2.2.1. CCTV Video Switcher Keyboard. The keyboard has two displays, a numeric keypad, and four function keys. The display shows “Monitor” and “Camera”. The monitor display is a three digit display that shows the monitor that the keyboard is currently controlling. The camera display is a four digit display that shows the number of the camera being viewed on the monitor that it is controlling.

1.2.2.1.1. Numeric Keypad. Digits 0-9 are general purpose keys used to enter numeric data. Operator will use the keypad to input monitor and camera numbers. “CLEAR” key reinitializes the keyboard; allowing the operator to clear incorrect data. If there is no data in the display, this key will place they keyboard to the default state. “ENTER” key terminates commands and indicates the end of data entry.

1.2.2.1.2. Function Keys. “MONITOR” key connects the keyboard to the desired monitor. Operator will utilize numeric keypad and enter monitor number. “CAMERA” key will call-up the desired camera to the selected monitor. Operator will utilize numeric keypad and enter the camera number. “NEXT” and “PREVIOUS” will switch cameras on the selected monitor.

1.2.3. AECS. Provides automated and manual access control through authorized entry and circulation control of authorized personnel and vehicles within limited and exclusion areas, as well as, monitors all IDS equipment associated with KUMMSC.

1.2.4. Lynx Predator Elite. Automated Entry Control System software designed to integrate IDS, AECS, CCTV subsystems, and the Wide Area Detection System (WADS).

1.2.5. Security Workstation. Provides complete operational control of the site intrusion detection system. The workstation provides the operator the capability to interact with the IDS, displays a graphic map depicting the layout of the facility, and provides audio/visual indication of alarm states. The workstation also provides access/control to the facility controlled by the operator/controller.

1.2.5.1. LPE Desktop. Dedicated to the LPE toolbars and associated utilities that facilitate operator interaction with the IDS/AECS.

1.2.5.2. (DCNI) Graphics Display Monitor (GDM). Provides visual indication of alarm states and communication states on a graphically displayed map in relation to KUMMSC, as well as, depicts states of portals and allows operators to interact with IDS/AECS.

1.2.5.3. Alarm Acknowledgement Plunger. A monitor device type that when depressed, acknowledges all incoming alarms.

1.2.5.4. (DCNI) Duress Switch. The duress switch allows an operator the ability to covertly communicate a situation of duress to security personnel operating within a separate security control center. KUMMSC Entry Control Point (ECP) operates three, Site Security Control Center (SSCC) operates three, Munitions Control (MC) operates two and the Base Defense Operation Center (BDOC) operates one. NOTE: This duress switch capability also exists at A and B-Side Maintenance Bays, Munitions Armory, Weapons System Security Squadron (WSSS) Armory, and the Enrollment Center. Duress from these locations will annunciate at every control center.

1.2.5.4.1. Upon duress activation, the security workstation is either automatically or manually disabled. ECP and MC are automatic and SC/AM/SCS are manual, refer to paragraph 3.6.6. When LE desk activates duress their system does not get taken by the SSCC. The SSCC will contact the LE Flight Chief via LE radio frequency and notify the LE Flight Chief of the current situation.

1.2.5.5. Standard Alarm Tone. An intermittent tone that generates upon receipt of an alarm.

1.2.5.6. Alarm Monitor Operator Status (AMOS) Tone. Alarms not acknowledged within 10 seconds from the Entry Control Point (ECP), Security Controller (SC), or Alarm Monitor (AM) workstation will generate an audible steady tone and subsequent alarm at the Security Control Supervisor (SCS) workstation. Alarms not acknowledged within 15 seconds from the SCS workstation will generate an audible steady tone and subsequent alarm at the Base Defense Operations Center (BDOC) workstation.

1.2.5.7. Local Display Area Operator (LDAO). The ECP, SC, and AM workstations are the primary Security Workstation for a sensored area.

1.2.5.8. Redundant Display Area Operator (RDAO). The SCS workstation has the same features as the LDAO and mirrors the functions by displaying alarm indicators, facilities, AECS status, map displays and other information that displays on the LDAO. This ensures system continuity should the LDAO fail. EXCEPTION: Topside WADS. Topside WADS are not mirrored from the LDAO to the RDAO through the AECS system.

1.2.5.8.1. Primary/Backup Panel Communication. Primary path of communication between Virtual Interface Panel-Enhanced (VIP-E) and Security Workstation is the LDAO. The Backup path of communication between the VIP-E and Security Workstation is the RDAO. When a LDAO receives a communication loss to one panel, all panels associated with that LDAO are automatically switched to backup path of communication. Panel communication must be manually configured to primary path after communication loss.

1.2.5.9. Remote AMOS Workstation. The BDOC workstation is not considered a RDAO, but is intended to receive alarms not acknowledged by operators at the Site Security Control Center (SSCC).

1.2.5.10. Enrollment Operator Station (EOS). Located at Pass and Registration, this workstation generates the Air Force (AF) Form 1199 Computer Generated (CG) Restricted Area Badge (RAB). This workstation is only connected to the Enrollment Master Station.

1.2.5.11. Enrollment Master Station (EMS). Located at Squadron Operations inside the Enrollment Center, this workstation (enrolls) authorized personnel's Personal Identification Number and Personal Identity Verification (Hand Biometric). A switch enables and disables communication between the EMS and the BDOC workstation.

1.2.5.11.1. Only personnel listed on the Enrollment Center Officials Authorization letter signed by the 377 WSSS/CC and 898 MUNS/CC may enroll badges and enable communication between the EMS and BDOC workstation. Additionally, enabling communication requires one 377 WSSS representative and one 898 Munitions Squadron representative.

1.2.6. (DCNI) Sensor. Part of the IDS that provides detection through volumetric or mechanical detection devices. Sensor equipment is capable of detecting the physical opening of entryways or movement within the specific area of sensor coverage. All sensors are fitted with tamper detection devices. Refer to Paragraph 1.3. for sensors specific to KUMMSC.

1.2.7. Hoffman Box. A metal enclosure that protects sensitive equipment from dust, dirt, oil, water, corrosion, and other contaminants. Field Distribution and Junction Boxes are examples of Hoffman Boxes.

1.2.8. (DCNI) Field Distribution Box (FDB). A tamper protected enclosure that groups IDS equipment and sensor inputs into a single or several Intrusion Detection Panel (IDP) and/or Portal Control Panel (PCP) located throughout KUMMSC and the surrounding areas. All FDBs are tamper protected. Refer to Attachment 3 for FDB locations.

1.2.8.1. (DCNI) Room 153. Protected by a Balanced Magnetic Switch (BMS) and DR301 Curtain Passive Infrared (PIR) device, this room is considered a FDB that contains network and communication devices critical to the operation of KUMMSC AECS. Two Hoffman enclosures located within Room 153 contain IDPs and PCPs. Access is controlled through an authorization letter signed by the 377 WSSS/CC and 898 MUNS/CC and two-person maintenance concept.

1.2.9. Junction Box. A tamper protected box located between a sensor and an enclosure, or a FDB and the operator workstation. These boxes allow access to the system hardware and are tamper protected or within a zone of protection, and secured with tamper proof screws.

1.2.10. Versatile Interface Panel (VIP)/Versatile Interface Panel-Enhanced (VIP-E).

1.2.10.1. The VIP is typically used for Security Workstations and associated equipment; console tampers, tones, duress switches.

1.2.10.2. The VIP-E is typically contained inside Field Distribution Boxes that enable communication between Security Workstations and IDS equipment/sensors. Four VIP-Es contained inside tamper protected boxes are also located above each Mantrap booth. VIP-Es are classified for their functionality; Intrusion Detection Panel (IDP) and Portal Control Panel (PCP).

1.2.10.2.1. Enhanced. VIP-Es have a network card that communicates with the Security Workstation via two 10/100 Megabyte (MB) ports for Primary (LDAO) and Backup (RDAO).

1.2.10.2.2. Monitor. A device that detects a change in state of the item it is monitoring. VIP-Es have sixteen channels used to connect monitor type devices. The card reader multiplexor (MUX) has seven monitor channels.

1.2.10.2.3. Relay. Opens and closes doors, controls lights, audible tones, and controls special functions. VIP-Es have eight channels used to connect relay type devices. The card reader MUX has three relay channels.

1.2.10.2.4. Serial Port. VIPs have two serial ports offering 1 channel per port for a total of 2 channels. Up to two devices (i.e. card reader or HGU) are hardwired into the VIP-E serial port. Card readers have the ability to be multi-dropped (connected to the serial port connection on a MUX). Up to 8 card readers can be multi-dropped.

1.2.11. Portal. A combination of devices such as Card Readers, Door Position Indicators (DPI), monitor points, and relays that allow authorized pedestrians or vehicles entry via the AECS.

1.2.11.1. Card Reader. Authorized personnel swipe their Kirtland Air Force Base (KAFB) 1199CG for entry and exit circulation control. These devices are tamper protected. A MUX, similar to a VIP, is located on the backside of the card reader for serial, monitor, and relay connections.

1.2.11.2. Hand Geometry Unit (HGU). Located at Mantrap 1 (M1) through Mantrap 4 (M4) booths. These are tamper protected and act as AECS Level 3 Personal Identity Verification (PIV).

1.2.11.3. Level 1 Portal. This level requires a Kirtland Air Force Base (KAFB) 1199 Computer Generated (CG) Restricted Area Badge (RAB) coded for the personnel and the card reader. Level 1 portals are automatic (no operator interaction) or manual (requires operator interaction).

1.2.11.4. Level 2 Portal. This level requires a KAFB 1199CG and Personal Identification Number (PIN). Level 2 portals have duress pin capability. All Level 2 portals are manual with the exception of V1AA which is not required to be a level 2 portal.

1.2.11.5. (DCNI) Level 3 Portal. This level requires a KAFB 1199CG, PIN, and metric. Level 3 portals have duress pin capability. M1-M4 booths are the only level 3 portals at KUMMSC. All level 3 portals are automatic (no operator interaction).

1.2.12. (DCNI) Discrete Controlled Area (DCA). A DCA is a secure area controlled by barriers and credential verification. Valid cardholders are tracked between DCA passages (they will always exit from one DCA and enter another). The AECS keeps track of how many cardholders are in a DCA in real-time. This enables operators to track personnel as they move throughout KUMMSC. Access to the DCA by an individual is determined at the time of badge enrollment. This ensures that personnel are only able to access areas for which they are cleared.

1.2.13. (DCNI) Power Sources. In the event of commercial power loss, KUMMSC has a standby emergency power source and uninterruptible power supply (UPS) capable of operating IDS equipment/sensors for a minimum of four hours. Upon loss of commercial power, 898 Munitions Control has a panel that indicates which type of power is being used.

1.2.13.1. Generator. Located inside the Utility Building behind Door 3, the generator automatically starts upon detecting loss of commercial power. All portions of the facility powered by commercial power will be operational. Automatic generator start up and full load pick-up is required within 65 seconds of commercial power being lost. If the generator does not automatically start all 377 WSSS flight personnel are trained on manual generator start up procedures.

Refer to flight **Special Security Instructions, Scorpion 1, Attachment 6** for Manual Generator startup procedures.

1.2.13.2. (DCNI) Uninterruptable Power Supply. Two battery strings (String A and String B) are located within Room 160 and are constantly trickle charged by commercial power. KUMMSC UPS provides critical power to all sensors, cameras, workstations, FDBs, half of the loading dock lights and radio communication systems. Upon commercial and generator power failure, KUMMSC UPS will last a minimum of four hours. NOTE: Blast doors will only cycle approximately two and a half times on KUMMSC UPS. After blast doors cycle two and a half times, manual pumping procedures for opening blast doors will be applied. Manual blast door pumping procedures are located near every blast door.

1.2.13.2.1. (DCNI) FDBs located outside of the KUMMSC are provided with an UPS capability. Each FDB contains four batteries that last a minimum of four hours upon loss of commercial power.

1.2.14. Water Sensor. Device that detects moisture on the floor within the area they are deployed; in Maintenance Bay A/B and B10-B11.

1.2.15. Blast Containment Management System (BCMS). Notifies the Munitions Control Operator of a significant pressure change consistent with an explosion or blast within the affected zone, allowing them to button-up the facility or turn off individual air or water valves.

1.3. IDS Sensors. Sensors are classified as Volumetric (Motion Detection) or Mechanical (Point Detection). Passive Infrared (PIR) and Microwave sensors are both classified as volumetric. Balanced Magnetic Switch (BMS) sensors are classified as mechanical. Refer to Attachment 5 for additional sensor information.

1.3.1. Tamper Switch. A device that annunciates prior to internal components of IDS equipment or sensors being subject to spoofing, bypassing, or tampering.

1.3.2. Passive Infrared (PIR) Detection. Detects movement and temperature change within a sensors' field of view; both conditions must be met for alarm annunciation.

1.3.2.1. DR301 Curtain. Provides a wall-type field of view out to 35 feet and is tamper switch protected.

1.3.2.2. DR851 Area. Provides a 180-degree field of view out to 45 feet and is tamper chip protected.

1.3.2.3. ELTEC 862-71 Telescopic. Provides a beam-type field of view out to 500 feet and is tamper switch protected by a microtamper chip located on the back.

1.3.2. Microwave Stereo Doppler (SD) Detection. Detects object movement within a sensor's field of view.

1.3.2.1. SD80. Provides a field of view of 80x80 feet and is tamper switch protected.

1.3.2.2. SD150. Provides a field of view of 150x40 feet and is tamper switch protected.

1.3.3. Balanced Magnetic Switch Detection. Detects the physical opening of doors, windows, or gates and is tamper switch protected.

1.3.3.1. Door Position Indicator (DPI). A tamper protected BMS device that is used to indicate the position of doors, vehicle gates/barriers, and blast doors. Intrusions associated with DPIs require only CCTV IVA and not an armed SF response. These devices are also not required to be sensor tested and are used only as indicators.

1.4. Operator Responsibilities.

1.4.1. Sensor Testing. Electronic Security Systems (ESS) staff conducts Performance and Evaluation and Vulnerability Tests to ensure proper operation of IDS. Vulnerability tests are conducted to identify and mitigate system vulnerabilities, ensuring the system continues to detect and assess intrusions effectively. These checks will be documented in the AF Form 53, *Security Forces Blotter*.

1.4.1.1. Prior to sensor testing, ESS NCO will notify LDAO and RDAO of sensor testing initiation. Operators will ensure at least two authorized maintenance personnel and one ESS S3 staff is on-scene during the course of sensor testing.

1.4.1.2. Once alarm is received, the operator will ensure the ESS staff can hear the alarm annunciate over the radio/stentofon and gives the time, type, description and location of the alarm unless otherwise specified.

1.4.2. (DCNI) Booth Checks. KUMMSC Entry Controllers (KEC) are responsible for booth operational checks every shift. The Senior KEC will ensure all seven invalid cards are used for attempted entry at M1-M4 booths. These checks will be documented in the AF Form 53.

1.4.3. Duress Checks. Following shift change, the duress checks will be initiated with the SF Armory, ECP, MC, SC, AM, SCS and BDOC. SSCC, ECP, MC, and BDOC will stay in constant contact via intercom or landline throughout the entire duration of duress checks. Once the SF Armory completes their checks, personnel are no longer required to stay in contact with the control centers. These checks will be documented in the AF Form 53.

1.4.3.1. Personnel will only activate the duress alarm under direction of the SCS, at no time will more than one duress alarm be activated at one time.

1.4.3.2. Ensure the duress alarm is received at every terminal with proper audible and visual indicators. BDOC must verify that MC was disabled via the system status after activation of duress. BDOC will re-enable MC prior to additional duress testing and verify via system status.

1.4.4. Daily Sensor Testing. Area Supervisors (AS) or Flight Chiefs/Flight Commanders (FC/FCC) will conduct daily sensor testing. These checks will be documented in the AF Form 53, *Security Forces Blotter*.

1.4.4.1. Entry and Exit Vehicle Tunnels. AS or FC/FCC will conduct walking tests of the Entry and Exit Vehicle Tunnels each shift to verify correct operation.

1.4.4.1.1 Subject will position themselves at V3 or V7 facing towards the loading dock.

1.4.4.1.2 Subject will make three intrusion attempts per likely avenue of approach (one from the left, middle, and right sides of the tunnel).

1.4.4.2. Perimeter Surveillance Radar System. Topside area supervisor or Flight Chief will conduct sensor test for the PSRS. Security Controller will refer to the posted PSRS test schedule for test type and location. The intruders objective is to enter the below ground area at the entry or exit ramp. The PSRS must detect (track) and assess (Slue to Queue) prior to the intruder gaining access to the entry or exit ramp. Mid shift PSRS sensor testing will test thermal imager capability. These checks will be documented in the AF 53, *Security Forces Blotter*.

1.4.4.2.1. Utilize sensor testing checklist for correct procedures (QRC #G-3).

1.4.5. AECS Operator Proficiency Exercises. AS or FC/FCC will conduct random unannounced checks of LDAO, RDAO and Remote system operators alarm assessment capabilities by causing actual sensor alarms. To guard against single insider manipulation of the sensor system, conduct an independent follow-up to verify alarm conditions. EXAMPLE: If AS or FC/FCC causes an alarm and terminates prior to an actual SF response; continue to provide dispatch upon termination. These checks will be documented in the AF Form 53, *Security Forces Blotter*.

1.4.5.1. AM. AS or FC/FCC must sign out key from MC for any proficiency exercises associated with Room 148, 158, or 160.

1.4.5.2. SCS. AS or FC/FCC will conduct proficiency exercises for the SCS to simulate conditions under which the RDAO would assume duties as the primary.

1.4.5.3. BDOC. AS or FC/FCC will conduct proficiency exercises for the BDOC to simulate conditions under which the remote would receive alarms not acknowledged by operators at the SSCC. AS or FC/FCC will contact SSCC and have the controllers AMOS the alarm sent by AS or FC/FCC to the remote location (BDOC) to ensure BDOC controllers annunciate and dispatch correctly. AS or FC/FCC will conduct proficiency exercises on all rooms and escape hatches randomly. (The AS or FC/FCC will not conduct the same proficiency exercise multiple times in a row. Checks are documented in the blotter to ensure proficiency exercises are being conducted properly.)

1.4.6. Sensor Maintenance. Prior to conducting maintenance to include sensor testing, personnel must be listed on the Sensor Maintenance Authorization letter signed by the 377 WSSS/CC and 898 MUNS/CC located in SSCC. SSCC will verify names of individuals performing maintenance in conjunction with the sensor maintenance authorization letter. Prior to completion of maintenance or closure of an unscheduled Priority 1 (P1), Priority 2 (P2), or Priority 3 (P3) work order, any alarm that is generated during maintenance must be tested in accordance with sensor testing procedures.

1.4.6.1. Only authorized maintenance personnel may conduct line fault and tamper tests with an authorized two-person maintenance concept; SF personnel will be present for all tests conducted. Refer to Attachment 6 for SF operational test procedures.

1.4.6.2. EXAMPLE: Two maintenance personnel conduct maintenance on a card reader and a card reader tamper alarm annunciates at the ECP. They tighten the connection and remount the card reader. One maintenance personnel will slowly lift the card reader to cause a tamper alarm. SF observing will ensure the alarm annunciates prior to an individual having the opportunity to gain access to spoof, bypass, or tamper with the internal parts of the card reader. SF will then swipe a valid 1199CG to ensure correct operation.

1.4.7. False and Nuisance Alarm Rate. Operators must ensure any portion of the IDS does not exceed invalid alarm rates. The term invalid alarms incorporates false and nuisance alarms. Controllers have access through the AECS to pull reports of all alarms within the last 24 hours, and beyond if needed, to ensure alarm rates have not exceeded the limit.

1.4.7.1. False Alarms. Alarms for which no cause can be determined.

1.4.7.2. Nuisance Alarms. Caused by an influence the sensor was designed to detect such as an animal, act of nature, or human, but not related to an intrusion. This influence must be clearly identifiable, short term, and followed by an immediate reset or it is considered a false alarm.

1.4.7.3. Interior IDS. No more than one false alarm and three nuisance alarms per sensor per month are acceptable, i.e., two false alarm in this area will generate an Air Force Technical Order (AFTO) Form 781a work order. Interior IDS is defined as sensors within B7/B14/B15 and B5 and B6 escape hatch sensors.

1.4.7.4. Exterior IDS. No more than one false alarm and three nuisance alarms per sensor per day are acceptable, i.e., two false alarms in 24 hours within this area will generate an AFTO Form 781a work order. Exterior IDS is defined as sensors outside B7/B14/B15.

1.4.7.5. Topside Wide Area Detection System (WADS) Alarm Rate. The false alarm rate for the topside WADS is ten per day, per sensor (STS-350 Ground Based Radar [GBR]).

1.5. Documentation.

1.5.1. Air Force Technical Order (AFTO) Form 781a, *Maintenance Discrepancy and Work Document*. Used and maintained by the AM to record all maintenance discrepancies on the IDS. Upon initiation of a P1, P2, or P3 Job Control Number (JCN), the AFTO 781a will document all required information in accordance with (IAW) Attachment 7. Refer to Attachment 8 for ESS compensatory measures and Attachment 9 for maintenance response times.

1.5.2. Alarm History. Records all alarm data (Valid, Nuisance, False) received at the Security Workstation. Operators will use computer generated LPE Alarm History Log or AF Form 340, *Sensor Alarm Data*, as directed by the ESS NCO. When utilized, the AF Form 340 will be initiated each day by the day shift operator; the AF Form 340 will be valid for a 24-hour period.

1.5.3. AFGSC Form 257 (Storage Igloo/Multi-Cubicle Opening/Closing Log). Operators will ensure they record all opening and closing of cells and maintenance bays on the AFGSC Form 257 daily. Operators will also ensure that SVA swaps are documented on this form as well. Munitions Control will provide SSCC with the MUNS Form 1 along with an estimated time of opening/closing into either the Cell Area or Maintenance Bay.

1.6. (DCNI) Unescorted Entry Requirements. Personnel must possess an AECS badge issued at KAFB with open area 8. These personnel do not require the assistant EC to be in the entrapment area prior to entry unless during FPCON Charlie or higher or Random Anti-terrorism Measures (RAM). The AECS badge contains badge number (located in the lower left corner) and appropriate KAFB Authenticator in the background. Personnel authorized to perform escort official duties will have the letter “E:” and the number corresponding to the area they are authorized to escort, below their picture on the front of the AECS badge.

1.6.1. Entry Procedures.

1.6.1.1. Personnel will pick up the outer gate phone, identify themselves, verify they are in possession of an AECS badge and state their security status.

1.6.1.2. Once allowed thru turnstile (T-3) place hand-carried materials through the x-ray machine. Then personnel will walk through the metal detector. If no alarm, proceed to the AECS booths. If alarm, proceed back through the metal detector, remove remaining metal objects and proceed back through metal detector. If on the second attempt, an alarm sounds, an EC will respond and hand-wand the individual requesting access.

1.6.1.3. Personnel will enter the booth and ensure the LOW SIDE door is closed. They will then present their AECS badge, enter PIN, and provide hand biometrics. Only one person is authorized in a single booth at a time. Personnel who attempt to put two or more personnel into a booth will be challenged and removed from the area.

1.6.1.4. During RAMs, the Assistant EC will check all hand-carried items and metal screen personnel entering/exiting for contraband. If an unauthorized item is found, the AS will be dispatched to determine whether or not malicious intent is evident. Contraband items will not be stored in the ECF/entrapment area for convenience.

1.6.1.5. Invalid Bio - Received when individual has three unsuccessful attempts at entering hand geometry. Invalid PIN – Received when individual has three unsuccessful attempts entering their personal identification number. For both incidents give the individual another chance to properly process through another booth. Upon the EC receiving two invalid Bio/PIN alarms:

1.6.1.5.1. EC will:

1.6.1.5.1.1. Immediately direct Assistant EC to the low side of the booths.

1.6.1.5.2. Assistant EC will:

1.6.1.5.2.1. Collect the individual’s identification **(RAB/CAC).** Compare the RAB and the CAC with the distributed copy of the MRABL and the PRAP log (Form 164). The MRABL will be generated every month by Pass & I.D. personnel. The MRABL will be place on the “(O:)” drive along with daily updates. Both the MRABL and the daily updates will be password protected. The password will be given to the Security Control Supervisor and Enrty Controller as needed.

1.6.1.5.2.2. If the individual is authorized after both forms of identification have be verified then the individual will be granted access to the facility. Allow access by unlocking one of the four booths and brief the individual they are to report to the Enrollment

Center and correct the issue (PIN/BIO Reset) with an Enrollment Center Official as soon as possible.

1.6.1.5.2.3. If an individual is unauthorized due to non-current MRABL, then the individual will be escorted out of the area by having the Assistant EC reverse Turnstile-3. Assistant EC will brief the individual to contact the EC before entering the facility to ensure daily updates have taken place.

1.6.1.6. Unauthorized Entry Attempts: Incorrect Credential, Altered Documents, Duress PIN.

1.6.1.6.1. EC will:

1.6.1.6.1.1. Immediately direct Assistant EC to the personnel entrapment area and initiate a challenge.

1.6.1.6.1.2. Purge the entrapment area(s) for personnel, if appropriate.

1.6.1.6.1.3. Notify SSCC and AS.

1.6.1.6.2. AS will:

1.6.1.6.2.1. Determine malicious intent.

1.6.1.6.2.2. Request additional SRTs as needed.

1.6.1.6.3. SSCC will:

1.6.1.6.3.1. Initiate a Security Incident if necessary.

1.6.1.6.3.2. Request a LE patrol if needed.

1.6.1.6.4. SRT will:

1.6.1.6.4.1. Provide over watch.

1.6.1.6.4.2. Once ESRT is on scene, escort individuals out of the sally port, collect all IDs and transfer custody to LE patrol if necessary.

1.6.1.6.4.3. Conduct of sweep of entrapment area and entry booth.

1.6.1.7. Manual Entry/Exit. Assistant EC must be posted in the entrapment area.

1.6.1.7.1. ALL Entry Booths Inoperative.

1.6.1.7.1.1. EC will:

1.6.1.7.1.1.1. Request permission to implement lockdown procedures from AS.

1.6.1.7.1.1.2. Direct Assistant EC to place (3) inoperable booths into lockdown.

1.6.1.7.1.1.3. All personnel entry credentials must be verified manually.

1.6.1.7.1.1.4. Ensure all entry/exit is annotated on the AF IMT 1109.

1.6.1.7.1.2. Assistant EC will:

1.6.1.7.1.2.1. Unlock booth 1 and allow entry/exit at the direction of EC.

1.6.1.7.1.2.2. Conduct personnel inspections as needed.

1.6.1.7.1.3. ONE Entry Booth Inoperative.

1.6.1.7.1.3.1. EC will place inoperative booth into lockdown and utilize operative booths for entry/exit procedures.

1.6.1.7.2. Turnstile Inoperative.

1.6.1.7.2.1. EC will:

1.6.1.7.2.1.1. Request permission to implement manual entry procedures from AS.

1.6.1.7.2.2. Assistant EC will:

1.6.1.7.2.2.1 Unlock turnstiles to allow entry/exit to entrapment area(s) at the direction of EC.

CHAPTER 2
ALARMS

2.1. (FOUO) Alarm Types. The following alarm types are associated with the LPE: SECURE, IN_ACCESS, INTRUSION, TAMPER, LINE_FAULT, AECS, DURESS, DISABLE, OVERRIDE, PRI_LOSS, PRI_RSTR, BCK_LOSS, BCK_RSTR, COMM_LOSS, COMM_RSTR, LOGON_FAIL, LE, SCS, MC, SC, AM, EC, TROUBLE, AC_FAIL, AC_RSTR, BATTERY, DROP_TRACK, IFF_ARMED, IFF_ACCESS, HOSTILE, NETWORK, VIDEO_LOSS, VIDEO_RSTR.

(FOUO) Table 2.0. - Alarms

Alarm Type	Alarm	Description
SECURE	Sensors	Sensor or equipment is in a normal state.
IN_ACCESS	Sensors	Sensor will no longer audibly and visually annunciate as an alarm upon an objecting breaking the field of view. Note: Tampers cannot be placed in access.
INTRUSION	Sensors	Object has penetrated the field of view of the associated sensor.
TAMPER	Sensor/Equipment	Possible removal of cover/faceplate or opening of door with the associated device.
LINE_FAULT	Sensors	Interruption in the communication between the sensor and panel.
AECS	Entry Requests	Cardholder credential verification at associated portal.
AECS	Process timeout, failed to open, lockdown, not properly secured, latch alarm	Portal alarms associated with doors, blast doors, turnstiles, and vehicle barriers.
AECS	DCA Violation	Cardholders DCA is not following the sequential order of DCAs within the system.
AECS	Cardholder Alarms	Refer to paragraph 2.2.

AECS	DPI intrusions	Separation of magnet and reed switch on a DPI.
DURESS	Workstations, duress capable locations	Activation of duress switch.
DISABLE	LE, ECP	LE or ECP camera disable.
OVERRIDE	Special function	Activation of special function.
PRI/BCK_LOSS	VIP-E (PCP/IDP)	Primary or Backup VIP-E communication loss.
PRI/BCK_RSTR	VIP-E (PCP/IDP)	Primary or Backup VIP-E communication restore.
COMM_LOSS	Multiplexor, HGU, Console VIP	Loss of communication to multiplexor, HGU, or Console VIP.
COMM_LOSS	PSRS GBR, PSRS Station, IFF Messenger	Loss of communication to PSRS GBR or STS Control Station.
COMM_LOSS	WSTI/LRTI Nexus Status	Loss of communication to WSTI/LRTI camera server.
COMM_RSTR	Multiplexor, HGU, Console VIP	Restore of communication to multiplexor, HGU, or Console VIP.
COMM_RSTR	PSRS GBR, PSRS Station, IFF Messenger	Restore of communication to PSRS GBR or STS Control Station.
COMM_RSTR	WSTI/LRTI Nexus Status	Restore of communication to WSTI/LRTI camera server.
LOGON_FAIL	Workstation	Operator failed to provide authorized credentials within three attempts to associated workstation.
LE/SCS/MC/SC/AM/EC	Workstation	Communication loss or restore between hosts and initializations.
TROUBLE	FDB temperature alarm	Temperature above 120 Fahrenheit.
TROUBLE	HI/LOW Pressure Alarm	Hydraulic pressure is above or below acceptable limits, notify MC.
TROUBLE	Water sensor	Detection of water, possible flooding.

AC_FAIL	Topside FDB, LE UPS, PSRS GBR	Loss of commercial power to associated equipment.
AC_RSTR	Topside FDB, LE UPS, PSRS GBR	Restore of commercial power to associated equipment.
BATTERY	Topside FDB, LE UPS, PSRS GBR, KUMMSC	Low battery indicated at 10% remaining. Associated FDB for PSRS GBR will annunciate a low battery alarm in such a case.
DROP TRACK	SC Workstation, *IFF DROPPED TRACK*	SC Workstation has accrued more than 1,000 track detections.
IFF_ARMED	PSRS GBR	GBR unit will detect tracks.
IFF_ACCESS	PSRS GBR	GBR unit will not detect tracks.
HOSTILE	*IFF OPR HOSTILE ASSESMENT*	SC tagged track hostile, annunciates at SCS workstation.
NETWORK	*IPSWITCH*	Network security alarm, notify CTS/ESS maintenance.
VIDEO_LOSS/RSTR	CCTV	CCTV camera video loss or restore.
Note: Alarm listing is not all inclusive		

2.2. Cardholder Access Denied Alarms.

2.2.1. MSC Block/Not in DB. Magnetic Strip Card/Not in Database occurs when a cardholder is in inactive status or does not have a card within the cardholder database.

2.2.2. No DCA access. Cardholder does not have proper assigned access group.

2.2.3. Invalid Pin. Cardholder has made 3 unsuccessful attempts entering a valid PIN.

2.2.4. Invalid Issue Code. Not used in current configuration.

2.2.5. Invalid Site Code. Card not issued at the installation.

2.2.6. Invalid Bio. Cardholder has made 3 unsuccessful attempts entering a valid hand biometric.

2.2.7. No Bio Template. Cardholder’s hand biometrics have not been inputted into the system (via enrollment).

CHAPTER 3
AECS SYSTEM OVERVIEW AND OPERATION

3.1. Operator Session. Consists of the Linx Predator Elite Desktop and Graphics Display Monitor. The Linx Predator Elite software has floating help over every icon. Operator can hover the mouse over an unknown icon to display its function. Most icons in LPE are universal and the same characteristics apply in each unique menu. The Linx Predator Elite desktop has three menus.

3.1.1. File. Allows the operator to log-in and log-out from the system. Only ESS NCO and System Administrators (SA) can exit the desktop display. Only those set up with operator credentials may log-in. Log-ins and passwords are workstation specific and passwords are changed every 55 days. Passwords are case sensitive and operators have three attempts to log-in. A third failed attempt locks out the workstation for one minute. Operators must log-out to exchange sessions with another operator.

3.1.2. Tool Bars. The name of the current toolbar appears at the top below the Main Bar, the default toolbar is the Runtime Toolbar. From this menu the operator can select the Editor Toolbar and Activity Reports.

3.1.3. Help. Displays generic help menu and current Linx Predator Elite version.

3.2. Runtime Toolbar. The Runtime toolbar is a split pane screen. The alarm monitoring utility is permanently docked in the top pane and can never be smaller than half the desktop (10 alarms). Advanced Process Definition (APD) shortcut buttons are located on the top right hand corner and unique to each workstation. The bottom split pane window is used to dock sub-menus indicated by the black arrow inside a white box; Administrative Messages, System Status, Cardholder Information. The session status bar indicates system information and allows operator interaction.

3.2.1. Connected. Status of connection to the host computer; Connected: SCS/AM/SC/ECP/MC/LE.

3.2.2. Operator. Login credential.

3.2.3. Online. Yellow/Offline indicates the workstation is not connected. Green/Online indicates the workstation is connected.

3.2.4. Alarm Bell. When the operator interfaces with another toolbar, the grey box turns into a shortcut icon for the Alarm Monitoring utility.

3.2.5. 0 Alarms. Displays the count of unacknowledged alarms; Red/Alarms, Green/No Alarms, Yellow/not connected.

3.2.6. Time/Date. Displays the current time and date.

3.3. Runtime Toolbar Sub-Menus.

3.3.1. Alarm Monitoring. Displays all alarms and cannot be exited. The sub-menu cannot be closed out and cannot be resized to less than 10 alarms displayed. The alarm monitoring sub-menu has five unique menus; Utilities, Queue, Fields, Sort Filter, Alarm Banner.

3.3.1.1. Utilities Toolbar. Twelve utilities for interacting and managing alarms.

3.3.1.1.1. Resume CCTV Call-up. Alarms with associated CCTV will automatically call-up video upon annunciation. If there are unsecured alarms in the queue, associated CCTV for alarms will not automatically display upon subsequent annunciation. Additional alarms with associated CCTV coverage will not be displayed unless this utility is executed.

3.3.1.1.2. Add Comments. Operator can add comments to a secured alarm. Operators can also retrieve canned entries, create canned entries, and delete canned entries.

3.3.1.1.3. Acknowledge All Alarms. Acknowledges all incoming alarms. If the number of alarms exceeds the display capability of the window pane (60+), this icon will acknowledge all alarms, even if they are not visible on the alarm queue.

3.3.1.1.4. (DCNI) Cardholder Information. If the highlighted alarm was associated with a card reader, this icon will display information about the cardholder that caused the alarm. NOTE: KUMMSC does not have any card reader generated alarms associated with this utility.

3.3.1.1.5. Alarm Detail. Brings up detailed information about the highlighted alarm. Operators can utilize this for the device number for search in the Hardware Map. Transaction and alarm number is also displayed to assist System Administrator and ESS Maintenance troubleshooting.

3.3.1.1.6. Acknowledge Single Alarm. Acknowledges a single alarm; alarm must be highlighted. Difficult to acknowledge multiple alarms using this utility.

3.3.1.1.7. Secure All Alarms. Action secures all alarms in the Alarm Monitoring queue; not available to operators.

3.3.1.1.8. Secure Single Alarm. Action allows operator to secure a single highlighted alarm with one of the three Alarm Tag types. Upon applying an alarm tag, radio button selection does not automatically reset, the last tag applied will be selected for all subsequent alarms.

3.3.1.1.8.1. Valid. Actual intrusion or authorized access (e.g., M1 invalid pin caused by personnel inputting the wrong pin, AM accessing a room/sensors).

3.3.1.1.8.2. Nuisance. A condition exists the sensor was designed to detect, but not related to an intrusion (e.g., Operator bumps console door and a console tamper annunciates).

3.3.1.1.8.3. False. No known cause.

3.3.1.1.9. Call-Up Graphics. Action will display the highlighted alarm on that GDM as a graphic representation. Not all alarms have a graphic representation.

3.3.1.1.10. Cancel All Un-Securable Alarms. Action will clear all alarms from queue, regardless of state; not available to operators.

3.3.1.1.11. Cancel Un-Securable Alarm. Action will clear a single alarm from queue, regardless of state; not available to operators.

3.3.1.1.12. Call-up VSS/CCTV. Action will display associated CCTV of the highlighted alarm. A "+" symbol indicates an alarm has associated CCTV. An "*" indicates an alarm is currently being viewed on the associated assessment monitors.

3.3.1.2. Sort Filter. Three options are available; alarm, pending and secure. Clicking the checkbox permits the operator to view or hide certain alarms. Only secured alarms can be hidden. Secure alarms will display up to a maximum of 72 hours.

3.3.1.3. Alarm Banner. The banner sits on top of the alarm monitoring fields and displays current unacknowledged alarms.

3.3.1.4. Alarm Monitoring Fields. Displays alarms in 7 sortable fields; Alarm Type, Alarm Description, Time/Date, Class (Classification), Prior (Priority), Tag, Status.

3.3.1.4.1. Alarm Type. 10 characters of defined alarm type (e.g., COMM LOSS, COMM RSTR, TAMPER, INTRUSION, DURESS).

3.3.1.4.2. Alarm Description. 30 character alarm description.

3.3.1.4.3. Time/Date. Time and date the alarm occurred.

3.3.1.4.4. Class (Classification). Three classifications of alarms; SECR/Security, NOTE/Notification, PROC/Procedural.

3.3.1.4.4.1. SECR. Classification associated with an alarm that indicates possible degradation of security or of the security system.

3.3.4.4.4.2. NOTE. Classification associated with an alarm that notifies the operator of a condition affecting the associated piece of equipment.

3.3.4.4.4.3. PROC. Classification associated with an alarm that indicates cardholder failed to follow proper procedure with associated access control equipment.

3.3.1.4.5. Prior (Priority). (1) Interior Intrusion, (2) Interior Tamper, (3) Exterior Intrusion, (4) Exterior Tamper, (5) AECS Access Alarms, (6) Duress, (7) Comm Loss/Comm Rstr and Topside Wide Area and Detection System (WADS), and (8-10) all other alarms.

3.3.1.4.5.1. Alarms that AMOS display as Priority "0" on the workstation that AMOS'd the alarm. The workstation that receives that AMOS alarm will display the original priority. Once an alarm has AMOS'd it can no longer be acknowledged by the original operator.

3.3.1.4.6. Tag. Valid, nuisance, or false tag that was applied when operator secured the alarm.

3.3.1.4.7. Status. Current status of alarms' state, alarms can be either Alarmed, Pending, or Secured.

3.3.1.5. Alarm Monitoring Queue. Displays all incoming alarms based on priority. Alarms have different colors and conditions. The different conditions are BLINKING and SOLID; unacknowledged and acknowledged.

3.3.1.5.1. Unacknowledged Alarms. RED and BLINKING.

3.3.1.5.2. Acknowledged Alarm. RED and SOLID.

3.3.1.5.3. Secured Alarm. GREEN and SOLID.

3.3.1.5.4. Duress Alarm. CONSTRUCTION ORANGE and BLINKING/SOLID.

3.3.1.5.5. Notification Alarm. BLUE and BLINKING/SOLID.

3.3.1.5.6. Workstation Re-Initialization. FOREST GREEN and BLINKING/SOLID.

3.3.2. Administrative Messages. Displays real-time transaction activity occurring on the AECS LPE. The system generates two types of transactions; host generated and panel generated. Host generated transactions are system related events. Panel generated transactions are related to panels and associated devices. LPE generates 256 possible transactions and additional WADS transactions (256+), but only 1000 will display in the Administrative Messages sub-menu. All alarms have an associated transaction, but not all transactions have an associated alarm.

3.3.2.1. Continue/Pause. Selecting the "Pause" radio button will stop the scroll bar from moving with the transactions as they occur. Transactions still occur and display, but do not flow through the *Administrative Messages* sub-menu. Selecting the "Resume" radio button will push the scroll bar to the bottom as the next transaction occurs.

3.3.3. System Status. System Status sub-menu displays the current status of all system components related to the applicable workstation. All information is dynamic and real-time, known as self-polling. As the RDAO, the Security Control Supervisor workstation has the ability to view status of all devices.

3.3.3.1. Navigation. System Status utilizes a split pane window; one for Display Criteria (search criteria) and System Status Device List (search results). System status is sortable by field.

3.3.3.2. Searching. The search bar is located on the top pane and has six utilities; Save, Edit, Sort Filter, Search, Request Status, Request Status All.

3.3.3.2.1. Save. This utility is not required to initiate search.

3.3.3.2.2. Edit. Operator will select this utility prior to selecting search criteria.

3.3.3.2.3. Sort Filter. Once operator inputs search criteria, this utility is used to return search results.

3.3.3.2.4. Search. Binoculars located near the search bar field. This utility is used to search for items in the search results.

3.3.3.2.5. Request Status. Request status of a single, highlighted device.

3.3.3.2.6. Request Status All. Request status of currently displayed devices.

3.3.3.3. Search Criteria. Operator utilize Primary Display Criteria, Display Mode, and Display action for searching. Operators will “Sort Filter” once “Display Mode” (Search Criteria) has been selected by operator. There are five primary search displays available, with several sub-displays.

3.3.3.3.1. SYS ID. Each workstation has a unique System number; (0) All hosts, (1) LE, (2) SCS, (3) MC, (4) EC, (5) SYS ADMIN, (6) AM, (7) SC.

3.3.3.3.2. NUMBER. This is the only search function that displays after selecting the “Sort” radio button and subsequently selecting “Sort Filter”. This will display devices associated with the workstation by device number, in chronological order. All devices have a unique number (also displayed on “Alarm Detail”). Different device types may have the same number, but devices of the same type will not.

3.3.3.3.3. DESCRIPTION. Up to 10 characters can be entered when using this display mode. This is a sliding search, meaning that any pattern entered will be searched within an entire record. If B1 is entered with no space, the search results will return all devices with the description B1, e.g., B1, B10, B11, B12, B13, B14 etc. Entering B1 with a space will return devices with B1 in the description only, e.g., B1, B1 card reader, B1 card reader TMP.

3.3.3.3.4. DEV TYPE. Displays devices based on type. As the redundant backup display (RDAO), the SCS will see all devices associated with lower nodes. Operator cannot request status of LINX Panels, Host, Host Comm, and DCA.

3.3.3.3.4.1. LINX. Displays all LINX (PCP/IDP, Host Panel, card reader panel) panels associated with the workstation. Cannot request status of this device. Note: The SCS will display VIP-E primary and backup panels for all workstations.

3.3.3.3.4.2. MONITOR. Displays all monitor devices types associated with the workstation.

3.3.3.3.4.3. RELAY. Displays all relays associated with the workstation.

3.3.3.3.4.4. READER. Displays all card readers associated with the workstation. These are displayed as a device and separately than the LINX PANEL associated with the card reader.

3.3.3.3.4.5. ELEVATOR. Not used.

3.3.3.3.4.6. HOST. Displays the workstation host.

3.3.3.3.4.7. DCA. Displays all DCAs associated with the LPE. The DCA count is dynamic and in real-time.

3.3.3.3.4.7.1. NON-CONTROLLED. AECS does not track cardholders.

3.3.3.3.4.7.2. (DCNI) NO-LONE. DCA cannot have a single occupant, KUMMSC is listed as "NO LONE" as the highest level of access control. Note: When an operator grants access to any two-person area blast door, AECS will move the first cardholder that swipes into the applicable DCA. If the process does not complete (process timeout, failed to open), the second cardholder will not be switched, but the first cardholder will remain in the two-person DCA. The operator must manually switch the first cardholders DCA back to swipe again.

3.3.3.3.4.7.3. STANDARD. DCAs operator normally, granting access based on a cardholders' DCA authorizations (Non-Two Person Access, Area 8, or ALL Access). AECS tracks cardholders and controls entry/exit.

3.3.3.3.4.7.4. STANDARD NO-CNTL. DCA tracks cardholders at specific portals, but does not track cardholders in other areas.

3.3.3.3.4.8. HOST COMM. Displays host to host communication. SCS will show host to host communication with all lower and higher nodes. All other workstations will display Primary to SCS and Backup to LE.

3.3.3.3.4.9. PORTAL. Displays all devices associated with the portal.

3.3.3.3.4.10. ALARM KEYPAD. Not used.

3.3.3.3.5. DCA. Displays a single DCA, but cannot display all DCAs.

3.3.3.4. Fields. There are 7 unique fields that are sortable, similar to the Alarm Monitoring sub-menu. A sort criterion is displayed on the title bar located on the lower split pane.

3.3.3.4.1. SYS ID. The host number associated with the device.

3.3.3.4.2. NUMBER. Unique number associated with the device type.

3.3.3.4.3. DESCRIPTION. Detailed description of the device type.

3.3.3.4.4. DEV TYPE. Refer to Paragraph 3.3.3.3.4., *DEV TYPE.*

3.3.3.4.5. DCA. DCA area of associated device.

3.3.3.4.6. DCA CNT. Number of cardholders in the associated DCA (Dynamic and Real-Time).

3.3.3.4.7. STATE. Device types have two states, Normal (N) and Not-Normal (NN). The color identifies the device STATE and text defines the CONDITION. Normal state is typically green and not normal state is typically red.

3.3.4. Cardholder Information. Cardholder Information sub-menu allows operators to access cardholder information. This sub-menu has minimal editing for operators based on authorization rights. Only the SCS has the ability to change a cardholders access to "Inactive" or "Active". The SCS also has the ability to edit personnel category to "All Access" or "Admin Area".

3.3.4.1. Cardholder Search. All operators can search for cardholders utilizing three methods: (1) clicking the previous and next icons, (2) entering cardholder stamped ID and clicking find, (3) find icon.

3.3.4.1.1. Find Icon. The find icon is located on the top right hand corner of the search screen. The initial prompt will alert the operator that only the first 500 cards display. If the badge number is over 100501, the search will not return a result. The operator must select the first letter of the last name in order to search for cardholders with a stamped ID of over 100501.

3.3.4.2. INACTIVE/ACTIVE. Operator must select "Edit" icon, then click "INACTIVE" or "ACTIVE". Operator must click the save icon to submit changes.

3.3.4.3. Change DCA. Operator can view which device the cardholder last swiped at under the "Last Accessed" title bar and change DCAs. The operator will click the current DCA and a dialog will display allowing any desired DCA to be selected. This action does not require save to function.

3.3.4.4. Assigned Access Groups. These are configured during badge generation at Pass and ID (EOS). There are three access groups that determine which areas the cardholder can access: (1) All-Access that allows personnel DCAS 59-70, (2) Non-Two Person Access that restricted access to DCAS 62-70,

(3) Area 8 that is used for both All-Access/Non-Two Person Access and non DCA badges (contractors).

3.3.5. Manual Command and Control (MRO). Used to run processes normally conducted on the Graphics Display Monitor. There are three menus that require operator input to function: (1) Device Type, (2) Number, (3) Command. Operators have access to Portal, DCA, CCTV, and PSRS device types. Number is associated with the unique device type ID. Command option calls-up a list of manual command options for the device type. After the configuration is set, operator must click “RUN” at the top left hand portion of the MRO sub-menu.

3.3.5.1. Portal. This manual command allows the operator to grant access to a desired portal. Operator will select the portal (e.g., B1, B2, B3, or B4) under the “Number” list help dialog and then “Grant Access” under “Command”. Operator will utilize APD shortcut buttons located at the top right hand corner of the runtime toolbar.

3.3.5.2. DCA. This manual command is used to reset/clear a DCA count displayed in “System Status”. Operator will select the desired DCA under the “Number” list help dialog and then “Reset Area” under the “Command”.

3.3.5.3. CCTV. This manual command is used to manually switch CCTV. This manual command requires two “RUN” commands to function. Unlike other MROs, the operator must select the “Command” dialog first. Operator will select monitor under “Command”, then select the desired monitor under “Number”. Operator will hit the “RUN” command. After the monitor has been selected (displays as a transaction), the operator will select, “Select Camera” under the “Command” list help dialog. The operator will then select the desired CCTV camera under “Number” and click the “RUN” command.

3.3.5.4. PSRS. This manual command is used to “ARM” and “STANDBY” PSRS units. Select the PSRS under the “Number” dialog and either “ARM UNIT” or “STANDBY” under “Command”. Operator must click the “RUN” command.

3.3.6. Dynamic Tracking. Monitors the activity of specific cardholders or readers. When criteria is set, a dialog displays cardholder information. Operator must close the dialog for subsequent tracking to appear or select the green traffic light button. The dialog displays Name, Stamped ID, Time/Date of Access, Transaction, Reader, and Access Group. Operators can track a single cardholder through all portals, a cardholder through a specific portal, or all cardholders through a specific or multiple portals.

3.3.6.1. Individual Cardholder, All Portals. Cardholder Tracking on, Device Tracking off.

3.3.6.2. Cardholder, Specific Portal. Cardholder Tracking on, Device Tracking on. Operator must select readers or portals utilizing the “Reader Device Help” or “Portal Device Help” icons.

3.3.6.3. All Cardholders, Specific Portals. Cardholder Tracking off, Device Tracking on. Operator must select readers or portals utilizing the “Reader Device Help” or “Portal Device Help” icons.

3.3.6.4. After selecting an “Active Time Interval”, Dynamic Tracking will function for 12 hours per save. Operator will select all transaction codes and “SAVE” after desired criteria is met.

3.4. Editor Toolbar. The Editor Toolbar is the second of three toolbars utilized by the operator. Operators have access to two sub-menus in this toolbar: (1) Hardware Map, (2) Process Editor. The hardware map is used during troubleshooting of system malfunctions and process editor allows operators to view system logic when an Advanced Process Definition (APD) fails to initiate.

3.4.1. Hardware Map. Displays the communication path of devices attached to panels. The hardware map defines the entire physical field device infrastructure as a visual representation of how devices are attached to LINX Panels and Panels to Hosts.

3.4.1.1. Navigation. Three colors are associated with Hardware Map navigation: (1) Green, slot or channel is defined/used, (2) Yellow, current device tree is expanded, applicable to Serial Port 1 and 2, (3) Grey, slot or channel is not defined/not used.

3.4.1.1.1. Monitor. Displays an expanded-view dialog when clicked, includes all monitors associated with VIPs or VIP-Es (e.g., BMS, PIR, Microwave, Tamper, etc)

3.4.1.1.2. Relay. Displays an expanded-view dialog when clicked, includes all relays associated with VIPs or VIP-Es (e.g., Light Emitting Diodes (LEDs), Tones, Open/Close functions, etc).

3.4.1.1.3. Serial Port 1/2 Interface. Includes multi-dropped devices (labeled as address 1-8). Slots are yellow if the device tree is expanded to display a card reader VIP or HGU. Typically associated with card readers and associated hardware (e.g., intercom tamper, JBOX tamper, card reader tamper, credentials).

3.4.1.2. Searching. Searching requires the operator to click the binocular icon located on the top right hand portion of the screen. The subsequent dialog displays a list of device types selectable by radio button. The “Help” icon will call-up a dialog of all devices associated with the desired device type selected.

Once the device is found, operator will click the “Binocular” icon in the “Device Dialog” to select the device and display the communication path.

3.4.1.3. Read Monitor/Relay Device Path. Operator will read device communication path from the channel or FDB, e.g., Channel 2 of IDP 179 in FDB 11, Room F1; e.g., FDB 11, Room F1, IDP 179, Channel 2.

3.4.1.4. Read Multi-Dropped Device Path. Operator will read device communication path from the channel or FDB.

3.4.2. Process Editor. Operator will search for the APD or special function that failed to initiate and locate “LOGIC LIST” on the bottom half of the split-pane screen.

3.5. Activity Reports. Three sub-menu functions are available for use to the operator.

3.5.1. Transaction History Report. Used to track the transaction history using a specific time/date, device type, DCA or cardholder data. This sub-menu utility can assist the operator when troubleshooting system malfunctions or failures, false alarms and logic failures. Note: Time configuration is a 12 hour clock.

3.5.2. Alarm History Report. Used to track the alarm history data for a specific time/date, device type, alarm type, and alarm tag. Assists the operator in tracking alarms past the 72-hour timeframe that the alarm monitoring sub-menu is limited to. Note: The alarm monitoring sub-menu will not always display all alarms within the last 72 hours.

3.5.3. Evacuation Report. The Evacuation Report is critical to the operator for facility evacuation or shelter in place contingencies. This sub-menu utility populates a list of all cardholders and DCA location. Report configurations can be defined to generate all DCAs, groups of DCAs or single DCAs and saved for frequent generation. NOTE: Configuring a report with DCA 60 will include all active cardholders.

3.5.3.1. Operator will select “Edit” or double click the listed report to enable “Edit Mode”. Operator will select applicable DCAs utilizing the dialog box that populates after clicking the *New** button.

3.6. Graphics Display Monitor. Interactive real-time graphical module that represents site views and icons, site views are graphical representations of monitored/sensored areas.

3.6.1. Toolbar Menu Functions. Top toolbar displays 6 utility icons used for interacting with the GDM.

3.6.1.1. Help. Calls-up generic Linx Predator Elite help manual.

3.6.1.2. GDM Search. Allows operator to search for devices that have a graphical representation on the GDM.

3.6.1.3. Zoom to 100%/Cancel. Once selected, default zoom view will display.

3.6.1.4. Zoom Out. Once selected, each click on the map view will zoom out.

3.6.1.5. Zoom In. Once selected, each click on the map will zoom in.

3.6.1.6. Open File View. Opens list of all views applicable to the workstation, also known as the treasure chest.

3.6.2. Icons. Two icon types assist the operator on the alarm graphics; execution and navigation.

3.6.2.1. Execution Icon. Executes an action e.g., acknowledge, secure, start APD. All execution icons for IDS equipment and sensors have a floating help that displays the device type and unique ID. When the operator hovers over a device, the unique ID will display on the lower half of the screen. Clicking the icon will call-up a dialog box that will display the unique ID at the top of the list menu.

3.6.2.1.1. Advanced Process Definition (APD). A process that combines a series of actions to complete a certain function. Typically utilizes for portal "OPEN", "SECURE", and Special Functions. These icons are pastel in color.

3.6.2.2. Navigation Icon. Navigates to a sub-view and represents device status (inner box) and alarm state (outer box). Device status is related to system status colors and alarm state is related to alarm/pending/secure colors.

3.6.2.3 Icon Behavior. An unacknowledged alarm will display red and blink. An acknowledged alarm will display red and remain solid. When the alarm is secured, it will display green and solid.

3.6.2.3.1. Acknowledge Alarm. Upon alarm annunciation, a single click will display a list dialog that allows an operator to acknowledge alarm.

3.6.2.3.2. Secure Alarm. Once an alarm has been acknowledged, the operator can single click the icon to display the list dialog. Once "Secure" is selected, the operator must add a comment and tags to the alarm. Note: If more than a single alarm annunciated from the device icon selected, all alarms are secured and comment/tag is applied to all.

3.6.3. Portal Functionality. Operators grant access to portals via the Graphics Display Monitor (GDM). All portals and special functions require valid interlock conditions. Automatic portals (Level 1 only) do not require operator intervention. Manual portals require the operator to "Grant Access" or initiate "Open" APD. Refer to Attachment 10 for special functions, interlock logic combinations, and posting requirements.

3.6.3.1. Level 1 Portal. Cardholder swipes KAFB 1199CG.

3.6.3.1.1 Automatic Portals. D1, D2, T4, D11, D7, D12, D13. Cardholder swipes for automatic entry.

3.6.3.1.2. Manual Portal. B1, B2, B3, B4, B8 (high), B9 (high), B12 (high), B13 (high), B10 (high), B11 (high). Operator must "Grant Access". Cardholder swipes and operator receives a notification entry request alarm. Operator clicks the "Open" APD icon or utilizes the "B" APD shortcut buttons.

3.6.3.1.2.1. V3/V4/V5/V7/V8. Does not require "Grant Access". Requires valid interlock prior to clicking "Open" APD or utilizing "B" APD shortcut buttons.

3.6.3.1.2.2. V1AA/V1AB/T5. Cardholder swipes and operator receives notification alarm. Operator initiates "Open" APD or utilizes the "B" APD shortcut button. Note: V1AA/V1AB/T5 can be opened without cardholder swipe.

3.6.3.2. Level 2 Portal.

3.6.3.2.1. V2/V6. Cardholder swipes and PIN, operator receives a notification entry request alarm. Operator clicks the "Open" APD icon or utilizes the "B" APD shortcut buttons.

3.6.3.2.2. B8/B9/B12/B13/B10/B11/B15. Requires two valid cardholder swipes and PIN to open when entering from "LOW" side. Operator clicks the "Open" APD icon or utilizes the "B" APD shortcut buttons.

3.6.3.2.3. B7/B14 (High/Low). Requires two cardholders and valid PIN and dual authorization with Munitions Controller.

3.6.3.2.3.1. Both cardholders swipe and PIN, operator receives a notification entry request alarm.

3.6.3.2.3.2. Operator clicks "OPEN" APD or utilizes the "B" APD shortcut buttons.

3.6.3.2.3.3. Munitions Controller has 3 seconds to "GRANT".

3.6.3.2.3.4. Operator and Munitions Controller push red control buttons (B7/B14) within 3 seconds.

3.6.3.3. Level 3 Portal. M1, M2, M3, M4 booths requires the cardholder to enter on the "LOW" side of the booth. Cardholder will push "REX" button and door will unlock. Booths require valid cardholder swipe, PIN, and biometric template. Cardholder must swipe after each PIN failure up to three attempts.

Additionally, cardholder has three attempts to pass hand biometric. Upon successful swipe, PIN, and biometric, high side door of booth will unlock. Booths display a light emitting diode (LED) with three colors to indicate status.

3.6.3.3.1. Green. Indicates booth is ready for entry.

3.6.3.3.2. Yellow. Indicates booth is in use.

3.6.3.3.3. Red. Indicates booth is in lockdown.

3.6.4. Special Functions. All duress switch devices must be in a secure state, (e.g., AM cannot execute a special function if any AECS duress switch is active.) Refer to attachment 10 for Special Functions and required interlock logic. Operator clicks the “Activate” APD icon or utilizes the “B” APD shortcut buttons to activate the special function. Operator clicks the “Deactivate” APD icon or utilizes the “B” APD shortcut buttons to secure the special function.

3.6.5. Emergency Override. SCS override procedures bypass system door logic to open special functions or single blast doors/vehicle gates or barriers. This is conducted at the SCS terminal by a certified SCS Controller and Munitions Controller. System Administrator are notified immediately after this procedure is used and will change the password within 24 hours or the next duty day.

3.6.5.1. From the Two-Person Cell Unlocking Device (CUD) Box, SCS will retrieve the SCS override envelope and Munitions Controller will retrieve the MUNS Control override envelope. SCS will select the door or special function that required override from the “B” APD Shortcut buttons located on the Runtime Toolbar.

3.6.5.2. SCS will type “ono” in the initials box. SCS will have the MUNS controller turn away from the terminal and enter the SCS-half of the password.

3.6.5.3. SCS will face away from the terminal and allow the MUNS Controller to enter MUNS-half of the password.

3.6.5.4. When both halves of the password are entered, SCS will click the “APD Override” key.

3.6.6. Workstation Enable/Disable. Consoles are manually or automatically disabled by the parent workstation. Operator commands cannot be issued when the workstation is disabled. The disabled console does not indicate that it has been locked out; however the parent workstation will display a yellow icon as the disabled console on the host to host GDM communication status screen. If the system is rebooted, it maintains lockout status. Upon duress activation, workstations are automatically or manually disabled.

3.6.6.1. ECP. Automatic. The SCS must re-enable the workstation.

3.6.6.2. MC. Automatic. The BDOC must re-enable the workstation.

3.6.6.3. SC/AM/SCS. Manual, the duress switch must be active in order to disable SSCC's workstations. If the duress switch is active and the BDOC has not disabled SSCC, two-person area blast door APDs and special functions will not work.

CHAPTER 4
PERIMETER SURVEILLENCE RADAR SYSTEM (PSRS) OPERATIONS

4.1. Perimeter Surveillance Radar System. The PSRS consists of four Ground Based Radars (GBR), six Wide Area Surveillance Thermal Imagers (WSTI), one Long Range Thermal Imager (LRTI), the STS Control Station, Pacific Northwest National Laboratories Correlation Model, and the Security Controller Workstation Graphics Display Monitor.

4.2. STS-350 Ground Based Radar. The model series STS-350 GBR uses Doppler radar technology for line of sight targeting in a 360 degree circle out to 300 meters. The radar unit makes one revolution every second to track personnel and vehicles.

4.3. WSTI/LRTI. The WSTI/LRTI cameras are used for assessment capability in conjunction with the PSRS (WSTI), ground loops (WSTI/LRTI) and contingency operations (WSTI/LRTI). The Joystick Control Unit (JCU) is used for movement and operation of the WSTI/LRTI cameras. WSTI/LRTI cameras are automatically called-up or manually called-up. Automatic call-up occurs during PSRS track or ground loop sensor detection. Manual call-up occurs with operator interaction with the system. Clicking the WSTI/LRTI camera icon and selecting the monitor number on the pop-up menu will display the camera coverage. Refer to Attachment 2 for WSTI/LRTI locations.

4.3.1. Wide Area Surveillance Thermal Imager (WSTI). The model series, Sentry II WSTI consists of one camera with two imaging functions, daytime and thermal. The WSTI has an optimal assessment range of 350 meters for both imaging functions.

4.3.2. Long Range Thermal Imager (LRTI). The model series, T2 LRTI consists of two cameras with two imaging functions, daytime and thermal. The thermal imager has a lifespan of approximately 2000 hours and must be turned off when not in use. The LRTI has an optimal range of approximately 2 kilometers.

4.4. STS Control Station. The STS Control Station is located within Room 153 and processes information from the GBRs as detection tracks. The information is sent through the Pacific Northwest Laboratories Correlation (PNNL) software.

4.5. Pacific Northwest Laboratories Correlation (PNNL) Software. The PNNL software performs cross-radar sensor correlation, which reduces double tracks when an object enters dual covered areas. Additionally, the correlation model reduces false track detections to minimize operator assessments and interactions. The consolidated track movement data is sent to the SC workstation Graphics Display Monitor (GDM).

4.6. Ground Loop Sensors. Two ground loop sensors are associated with the SC workstation, Powerline Road adjacent to High Ball 2 and Munitions Haul Road adjacent to High Ball 4. The SC workstation will annunciate an alarm associated with these two ground loops to notify the operator of a vehicle crossing. At the direction of the ESS NCO, FCC, or FC, ground loops may be placed in access during peak traffic hours.

4.6.1. Ground Loop Sensor Testing. Ground Loop Sensors will be tested once daily by mid shift AS or FC/FCC. Testing will consist of three attempts to cross over the ground loop without being detected. The first attempt will be driving over the ground loop on the hardened surface, the second attempt will be trying to bypass the ground loop by going around the left side of the hardened surface off road and the third attempt will be trying to bypass the ground loop on the right side of the hardened surface off road.

4.7. Topside Camera Project (TSCP) Disable. A switch is located on the SCS workstation console labeled *TSCP Connected and TSCP Not Connected (x3).* Turning the switch to *TSCP Not Connected* will disable the communication between all topside FDBs associated with the PSRS system; FDB 20-26. The SC workstation will no longer receive track or ground loop detections and WSTI/LRTI camera imaging will be unavailable. The SC and SCS workstations will receive communication loss alarms with all associated panels. If the controller receives an IPSWITCH alarm (see para 2.1 Table 2.0 of this volume [page 17]), utilize WSTIs and/or patrol IVA to assess alarm and refer to QRC #G16.

4.8. Security Controller Workstation. The SC workstation consists of the LPE Desktop and GDM. The GDM functions as a geo correct map that resembles topside KUMMSC.

4.8.1. Joystick Control Unit (JCU). Contains a joystick for pan/tilt/zoom with focus collar, and seven usable buttons.

4.8.1.1. TV/IR. Switch from daytime imaging to thermal mode. The LRTI thermal imaging mode will be turned off when not in use. In thermal mode, operator must use the GDM icon to turn the LRTI thermal off. Clicking the LRTI will display a menu, operator selects *Camera Off*.

4.8.1.2. NUC. Auto focuses the camera when held down for more than three seconds.

4.8.1.3. Arrow Keypad. Up and down arrows zoom-in or out.

4.8.1.4. INV. Switches thermal imaging between white hot and black hot.

4.8.1.5. Menu Button. Calls-up menu screen for the WSTI/LRTI. Only System Administrators will access the WSTI/LRTI menu.

4.8.1.6. C. Clears selection or functions as back on the menu screen.

4.8.1.7. PRK. Park or shut off the camera. The LRTI must be turned off via the GDM.

4.8.1.8. SCN. Changes the rate of zoom for the keypad. Selecting the button will alternate between constant focus and focusing one zoom per touch.

4.8.2 GoTo GPS. This function will pan a particular camera to any location on the GDM. The camera must be called-up on a monitor first. Left click the camera icon and select *GoTo GPS* on the pop-up menu. Once the menu disappears, click the desired location on the GDM. Clicking on an additional icon located on the GDM will take the operator out of the GoTo GPS function.

4.8.3. Calculate distance. Calculate distance between two locations on the GDM. Left clicking on the initial location on the GDM will populate a menu, selecting Calculate Distance will start the calculation at that point. Moving the mouse to any location will calculate the distance to the second point, displayed on the bottom left corner.

4.8.4. PSRS Tracking. Upon an object entering the field of view for any GBR, the SC workstation receives an *IFF Native Hostile* alarm annunciation. The GDM will display a trail of red squares along the objects path, known as a track. The track must be tagged as hostile, friendly, or neutral. Due to numerous conditions, an object may generate several separate tracks requiring the operator to tag the object several times throughout one path.

4.8.4.1. Hostile. Tracks will display as a red square and annunciate an IFF Native Hostile alarm at the SCS workstation.

4.8.4.2. Friendly. Tracks display as a blue circle.

4.8.4.3. Neutral. Tracks display as a green diamond. (e.g. wildlife, hard rainfall)

4.8.5. Slue to Queue. When a track or ground based radar detection annunciates on the SC workstation, the nearest associated WSTI/LRTI automatically pans to the detection. If the detection is a track detected by the PSRS, the WSTI will follow the track until the operator identifies and tags the track. Selecting *Resume Automatic CCTV Call-Up* will enable WSTI automatic assessment for subsequent tracks. Additionally, the operator must select Resume Automatic CCTV Call-Up anytime the operator utilizes the joystick on the specified WSTI/LRTI. Manual operator of the cameras will place a 30 second hold on the camera where it will not automatically move unless Resume CCTV is used by the operators.

4.8.6. Arm/Standby Mode. A single or multiple GBRs can be placed in *Standby* mode or *Armed* mode. Left click a single GBR on the GDM to populate a menu and select *Arm Unit* or *Standby*. Clicking the IFF Messenger icon will an operator to place all GBRs in either an armed or standby mode.

4.8.7. Layers. Two types of layers are associated with the SC workstation, scratch layer and mask layer. A scratch layer is a graphic representation of an area and has no function. A mask layer is used to include or exclude track detections from a particular area. Only system administrators can edit or add a layer file.

CHAPTER 5
X-RAY MACHINE OPERATIONS

5.1. (DCNI) X-ray Machine. KUMMSC has inbound and outbound X-ray machines to scan all hand-carried items. The X-ray will be power on only during active scanning. The X-ray operator will stop the X-ray belt when not in use. Items too large, too heavy or open/unsealed liquid containers will be manually searched. Items exempt from search will not be searched manually or scanned with the X-ray. The inbound and outbound X-ray will be tested prior to shift change to ensure correct operation. Refer to Attachment 11 for X-ray testing procedures.

5.2. X-ray Machine Components. Two monitors and one control pad is associated with each X-ray machine.

5.2.1. Monitors. The X-ray machine utilizes dual monitors, “SCREEN 1” (color) and “SCREEN 2” (black and white). Both screens display a toolbar at the bottom of the monitors. “SCREEN 1” indicates the display mode; “SCAN Mode”, “ARCHIVE Mode” or “REVIEW Mode” (refer to 5.2.2.3.) on the lower right hand portion of the screen. “SCREEN 1” and “SCREEN 2” both indicate the display mode.

5.2.2. The Advanced Operator Control Pad (AOCP). The key switch located at the top right hand corner turns the AOCP power on and off. There are four control pad functions associated with the AOCP: (1) Touchpad and Display Mode, (2) Indicator Lights, (3) Image Processing, (4) Emergency Stop.

5.2.2.1. Touchpad and Display Mode. The touchpad functions similar to a traditional laptop computer. Double tapping the touchpad will act as “ENTER” in certain menus. Double tapping and holding after the second tape will function as a drag-and-drop mode.

5.2.2.1.1. Dark/Light. Operator presses “DARK” or “LIGHT” to transition between various shades. “DARK” increases screen contrast to show greater detail on less dense (organic) objects. “LIGHT” decreases screen contrast to see through dense (inorganic) objects.

5.2.2.1.2. Zoom-In/Zoom-Out. Operator presses the “ZOOM-IN” or “ZOOM-OUT” button and a curser will appear on the screen. The touchpad is used to move the cursor over the area of interest. Each press of the “ZOOM-IN” or “ZOOM-OUT” button increases/decreases the screen magnification.

5.2.2.1.3. Monitor Toggle. The buttons allow the operator to toggle between “SCREEN 1” and “SCREEN 2”.

5.2.2.2. Indicator Lights. POWER light indicates that the X-ray is powered up. X-ray light indicates scanning is in process, which means the X-ray generator is actively producing X-rays within the inspection tunnel.

5.2.2.3. Display Mode. "SCAN Mode", ARCHIVE Mode" and "REVIEW Mode" are the three types of display.

5.2.2.3.1. SCAN Mode. The right and left arrows on the AOCP correlate with the direction of the X-ray conveyor belt. Right on the inbound X-ray will move the belt forward; left on the outbound X-ray will move the belt forward. Left on the inbound X-ray will move the belt in reverse; right on the outbound X-ray will move the belt in reverse. Stop will terminate belt movement.

5.2.2.3.2. ARCHIVE Mode. This function allows the operator to review images that have been automatically stored on the X-Ray archive. Press the "REVIEW" button and a menu screen will display. Position the cursor on the selector dial and double tap the touchpad. Pressing the forward button on the AOCP will display images from oldest to most recent. Pressing the reverse button will display images from most recent to oldest.

5.2.2.3.2.1. The earliest available archived image is available on the very left most side of the dial. The conveyer belt must be stopped before using the "REVIEW" function.

5.2.2.3.3. REVIEW Mode. This function is a limited version of Image Archive, allowing the operator to review images scanned since the last log-in. Review mode will process images from newest to oldest.

5.2.2.4. Image Processing. This group of buttons allows the operator to change the color, sharpness and other attributes of an image in order to identify potential threats. Image processing is grouped into primary functions, secondary functions, "PICTURE PERFECT", and "ATOM". Primary functions can only be applied one at a time only. Secondary functions may be applied in combination with primary functions. The conveyor belt must be stopped before using any of the image processing functions.

5.2.2.4.1. Color Primary Functions. "Color", "Organic", and "Inorganic" are three primary functions associated with "SCREEN 1". Pressing the "Color" button at any time will bring the view back to normal.

5.2.2.4.1.1. Organic. Emphasizes organic materials and de-emphasizes inorganic materials. Organic compounds are produced by and are associated with living organisms. They are used in some of the most power and dangerous explosives such as C-4, TNT, and Semtex.

5.2.2.4.1.1.1. Displays in hues of orange to reddish brown. Denser items display in darker shades and very dense items are colored black.

5.2.2.4.1.2. Inorganic. Emphasizes inorganic materials and de-emphasizes organic materials. Inorganic compounds are created by non-living natural processes or human intervention such as steel, brass, or aluminum. Possible threats include guns, knives, shanks, and brass knuckles.

5.2.2.4.1.2.1. Displays in hues of green to blue. Shade is determined by an item’s density. Denser items display in darker shades and very dense items are colored black.

5.2.2.4.2. Black and White (B/W) Primary Functions. “B/W”, “B/W Reverse”, and “Pseudo” are the three primary functions associated with “SCREEN 2”. Pressing the “B/W” button at any time will bring the view back to normal. Highly dense objects are displayed in darker shades, the lowest density, air, is displayed as white.

5.2.2.4.2.1. B/W Reverse. Inverts an image that’s displaying in B/W so that it displays white on black. B/W reverse image processing may make some details more visible, which may identify a potential threat object more easily.

5.2.2.4.2.2. “Pseudo”. Displays a B/W image in colors. These colors are based strictly on screen brightness. Pseudo image processing may make some details more visible, which may identify a potential threat object more easily.

5.2.2.4.3. Secondary Functions. “Edge Trace” and “HI-PEN” may be combined with primary image processing.

5.2.2.4.3.1. Edge Trace. Edge sharpens the image by increasing the contrast between boundaries of light and dark objects.

5.2.2.4.3.2. HI-PEN. Lightens screen contrast and allows the operator to see through dense (usually inorganic) objects.

5.2.2.4.4. Picture Perfect. Normalizes and enhances texture and detail in both inorganic and organic images. To resume screening bags, you must first exit PP by pressing the “PICTURE PERFECT” BUTTON. “PICTURE PERFECT” does not work in conjunction with secondary functions or “ATOM”.

5.2.2.4.5. ATOM. Determines the atomic number of an item or the average atomic number of a selected area of a scanned image.

5.2.2.4.5.1. Operator presses the "ATOM" button and positions the cursor to the upper left corner of the area of interest. Operator will double tap the touchpad and mode the cursor to expand the box covering the area of interest. Once the operator lifts the finger from the touchpad, the atomic number will be displayed at the bottom center of the screen.

5.2.2.4.5.2. Common atomic numbers are: Graphic/carbon, 7; Water, 8; Aluminum, 13; Steel (iron), 26.

5.2.2.5. EMERGENCY STOP. The emergency stop will only be used if there is a jam within the X-ray. The emergency stop is located on the upper left corner of the AOCP. Pushing it down will stop all X-rays and the conveyor. To disengage, turn the knob clockwise until the knob pops back out to the "OFF" position.

5.3. (DCNI) X-ray Machine Operation. Only certified KUMMSC Entry Controllers will operate the X-ray machine. The following steps will be followed to ensure no contraband or prohibited items enter or depart the facility.

5.3.1. Operators will ensure the X-ray machine is not activated until personnel place all hand-carried items flat on the conveyor belt. The operator will activate the X-ray machine until the items are viewable on the monitor, but stopping the item before it leaves the X-ray chamber. Once the operator verifies all items are identified and determined authorized, the operator will move the items out of the X-ray.

5.3.2. Hand-carried classified material will be placed flat on the X-ray conveyor belt, moved into the chamber, scanned and reversed back to the individual. The operator will keep the X-ray activated for all outbound hand-carried classified material. In the event the X-Ray is in-op, an entry controller will search the material.

5.4. Interpretation of Data. Items passing through the Inbound or Outbound X-ray machines are classified as authorized, unknown, and unauthorized.

5.4.1. Authorized items are positively identified as neither prohibited or contraband.

5.4.2. Unknown items are any unidentifiable item. When scanning outbound hand-carried items ensure all items such as electronic circuit boards or unusual looking tools are closely scrutinized. Contact Munitions Control for authorization and clarification of questionable items.

5.4.3. Unauthorized items are positively identified as prohibited or contraband.

5.5. Response to Unknown or Unidentifiable Item.

5.5.1. (DCNI) Initiate ECP lockdown via AECS and notify SSCC.

5.5.2. (DCNI) KEC will identify the owner of the hand-carried item in question.

5.5.3. (DCNI) The owner will be asked to open or display the hand-carried item and KEC will visually identify the item to determine if the item is authorized or unauthorized.

5.5.4. (DCNI) Refer to checklist E-4 (Suspicious Item in X-Ray) for further guidance.

5.6. Response to Unauthorized Item.

5.6.1. (DCNI) Stop movement of the X-ray conveyor belt to maintain control over the unauthorized item.

5.6.2. (DCNI) Initiate ECP lockdown via AECS and notify SSCC.

5.6.3. (DCNI) All personnel within the immediate vicinity will be identified or challenged depending on the situation.

5.6.4. (DCNI) Refer to checklist E-4 (Suspicious Item in X-Ray) for further guidance.

5.7. X-Ray Machine Re-Boot Procedures. Instances where the X-Ray machine becomes in-op then the KEC will need to re-boot the X-Ray machine. For X-Ray re-boot procedures refer to QRC G-21 (X-Ray re-boot procedures).

CHAPTER 6

METAL DETECTOR AND TRANSFRISKER

6.1. Metal Detector Procedures. All visitors to the facility will process through the metal detector coming into the facility and going out of the facility. When the metal detector alarms, an Entry Controller will utilize the handheld trans-frisker to identify the cause of the alarm. Each shift is responsible to test the metal detector at the beginning of each shift. Refer to Attachment 12 for specific metal detector testing procedures. If contraband is found, refer to QRC E-1 (ECP Entry Denial).

MEIER.JAMES
.K.1155144617

Digitally signed by
MEIER.JAMES.K.1155144617
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=USAF,
cn=MEIER.JAMES.K.1155144617
Date: 2016.07.26 13:32:39 -06'00'

JAMES K. MEIER, Lt Col, USAF
Commander

ATTACHMENT 1
REFERENCES, FORMS, ACRONYMS

References

AFI 31-101, *Integrated Defense* (FOUO), 8 October 2009, IC3, 03 February 2016

AFMAN 33-363, *Management of Records*, 1 March 2008

DoD S5210.41M_AFMAN 31-108 V1/V2/V3 *Nuclear Weapons Security Manual*, 7 March 2013, AFGSCSUP 21 February 2014

Kirtland AFBI 31-101, *Kirtland Underground Munitions Maintenance Storage Complex Operations* (FOUO), 26 April 2012

Prescribed Forms

No forms are prescribed by this publication

Adopted Forms

AF Form 340, *Sensor Alarm Data,* 1 May 1995

AF Form 797, *Job Qualification Standard*, 17 August 2011

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

AF Form 1199 CG*, Air Force Entry Control Card*, October 2012

AFTO Form 781A*, Maintenance Discrepancy and Work Document*, 17 June 2002

AFGSC Form 257, *Cubicle Access Log*, March 2012

Abbreviations and Acronyms

AECS	Automated/Advanced Entry Control System
AF	Air Force
AFGSC	Air Force Global Strike Command
AFMAN	Air Force Manual
AFRC	Air Force Reserve Command
AFRIMS	Air Force Records Information Management System
AFTO	Air Force Technical Order
AMOS	Alarm Monitor Operator Status
ANG	Air National Guard
AOCP	Advanced Operator Control Pad
APD	Advanced Process Definition
AS	Area Supervisor
BCMS	Blast Containment Management System
BDOC	Base Defense Operations Center

BMS	Balanced Magnetic Switch
BPS	Battery Power Supply
B/W	Black and White
CCTV	Closed Circuit Television
CG	Computer Generated
CUD	Cell Unlocking Device
DCA	Discrete Controlled Area
DOD	Department of Defense
DPI	Door Position Indicator
EC	Entry Controller
ECP	Entry Control Point
EMS	Enrollment Master Station
EOS	Enrollment Operator Station
ESS	Electronic Security Systems
FC	Flight Chief
FCC	Flight Commander
FOUO	For Official Use Only
GBR	Ground Based Radar
GDM	Graphics Display Monitor
HGU	Hand Geometry Unit
IAW	In Accordance With
IDP	Intrusion Detection Panel
IDS	Intrusion Detection System
INOP	Inoperative
IVA	Immediate Visual Assessment
JBOX	Junction Box
JCN	Job Control Number
JCU	Joystick Control Unit
KAFB	Kirtland Air Force Base
KEC	KUMMSC Entry Controller
KUMMSC	Kirtland Underground Maintenance Munitions Storage Complex
LDAO	Local Display Area Operator
LE	Law Enforcement
LPE	Linx Predator Elite
LRTI	Long Range Thermal Imager

M1/M2/M3/M4	Mantrap 1/Mantrap 2/Mantrap 3/Mantrap 4
MB	Mega Byte
MC	Munitions Control
MRO	Manual Override
MSC	Magnetic Strip Card
MUX	Multiplexor
NCO	Non-Commissioned Officer
OI	Operating Instruction
OPR	Office of Primary Responsibility
P1	Priority 1
P2	Priority 2
PCP	Portal Control Panel
PIN	Personal Identification Number
PIR	Passive Infrared
PNNL	Pacific Northwest National Laboratories
PRAP	Personal Reliability Assurance Program
PSRS	Perimeter Surveillance Radar System
RAB	Restricted Area Badge
RAM	Random Anti-terrorism Measure
RDAO	Redundant Display Area Operator
RDS	Records Disposition Schedule
RTES	Remote Target Engagement System
SD	Stereo Doppler
SF	Security Forces
SSCC	Site Security Control Center
UCNI	Unclassified Controlled Nuclear Information
UPS	Uninterruptible Power Supply
VIP	Versatile Interface Panel
VIP-E	Versatile Interface Panel-Enhanced
VSS	Video Storage System
WADS	Wide Area Detection and Surveillance System
WSSS	Weapons System Security Squadron

ATTACHMENT 2
CAMERA LOCATIONS

Camera	Location	Camera	Location
1	V1AA	**33**	Command Entry
2	N/A	**34**	B15
3	N/A	**35**	Air Handler B10
4	Entry Ramp	**36**	Air Handler B11
5	V2 Entry Ramp	**37**	Behind B10
6	V3 Entry Ramp	**38**	Behind B11
7	Sally Port V5	**39**	A Interlock B8
8	Sally Port V4	**40**	A Interlock B7
9	Load Dock V5	**41**	A Side FDB 1
10	Load Dock	**42**	A Side South
11	Load Dock	**43**	A Side B8
12	Load Dock	**44**	A Side North
13	B-2 Load Dock	**45**	A Side South
14	Load Dock	**46**	A Side North
15	V6 Load Dock	**47**	A Bay B9
16	Exit Ramp V7	**48**	B Interlock B13
17	Exit Ramp V6	**49**	B Interlock B14
18	Exit Ramp V8	**50**	B Side FDB 3
19	Entry Portals	**51**	B Side South
20	Entry Portal	**52**	B Side B13
21	Exit X-Ray	**53**	B Side North
22	D-11 Enclosure 8	**54**	B-Side North
23	Entry Hallway	**55**	B Side North
24	Entry Hallway	**56**	B Bay B12
25	Entry Hallway B1	**57**	North East WSTI
26	Interlock B3-4	**58**	South East WSTI
27	Interlock B1-2	**59**	South West WSTI
28	Brandy Hall 7-14	**60**	North West WSTI
29	Brandt Hall B3-4	**61**	LRTI
30	B-6	**62**	Pad-5 WSTI
31	B-5	**63**	Route B WSTI
32	Command Room		

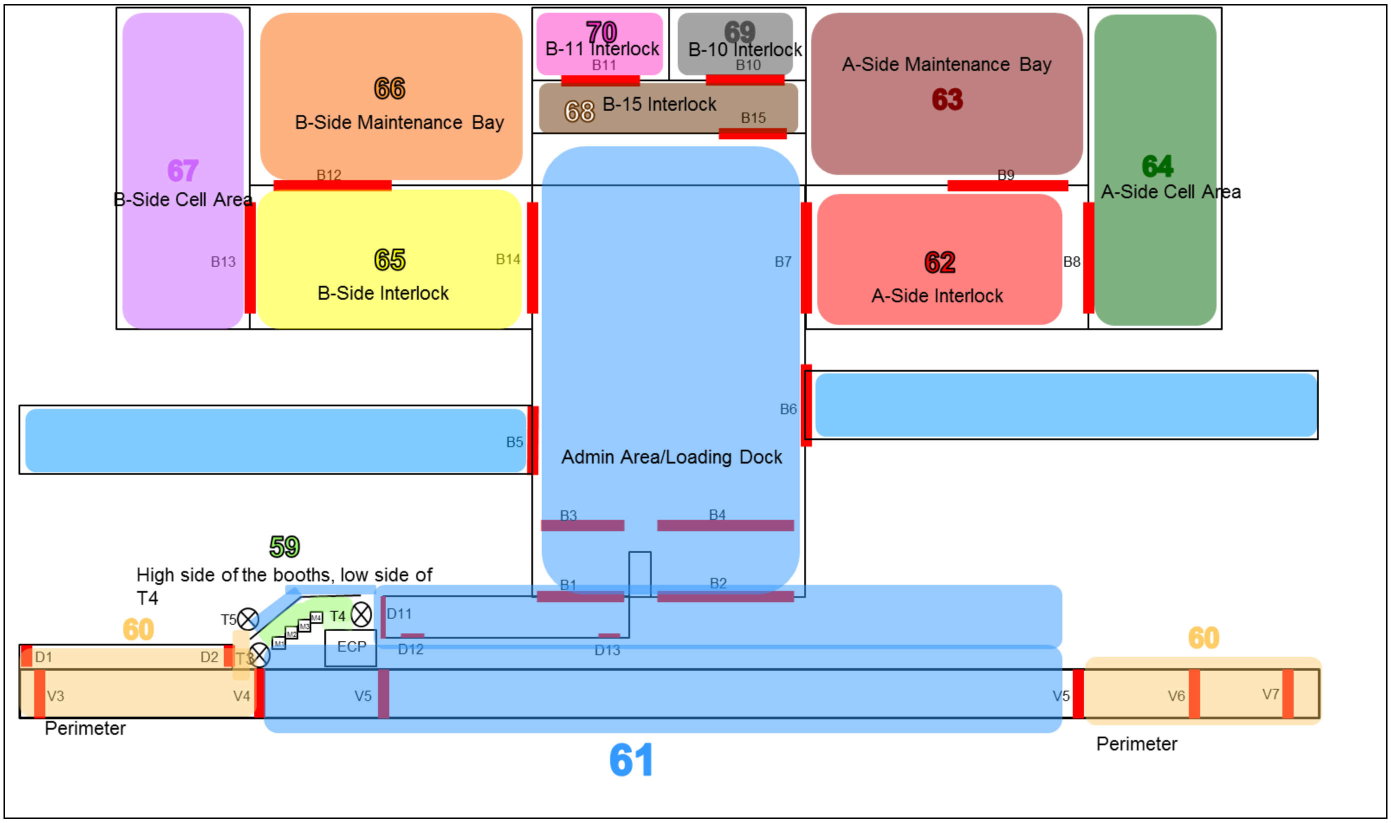
ATTACHMENT 3
FDB LOCATIONS

FDB Numbers and Locations	
FDB-1	A-Side Hallway North
FDB-2	A-Side Hallway South
FDB-3	B-Side Hallway North
FDB-4	B-Side Hallway South
FDB-5	A-Side Maintenance Bay
FDB-6	Room 123 Mechanical Room (B15 Low)
FDB-7	B-Side Maintenance Bay
FDB-8	Outside ECP (D11 Low)
FDB-9	Room 153
FDB-9a	Inside Room 153
FDB-9b	Inside Room 153
FDB-10	Utility Building Door 2
FDB-11	Room F1
FDB-12	Loading Dock
FDB-20	Northwest WSTI
FDB-21	Northeast WSTI
FDB-22	Southeast WSTI
FDB-23	Southwest WSTI
FDB-24	Highball-2 WSTI
FDB-25	Highball-4 LRTI
FDB-26	Pad-5 WSTI

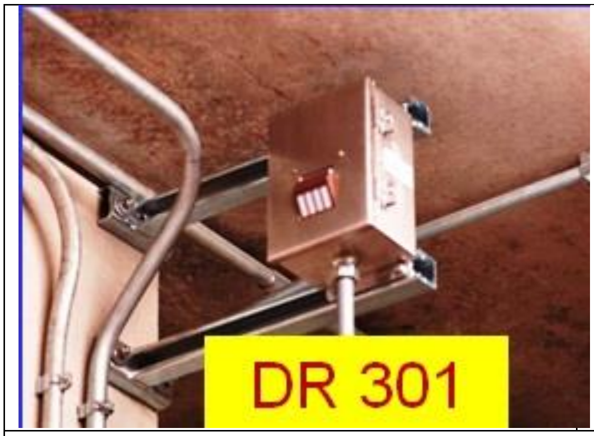
ATTACHMENT 4

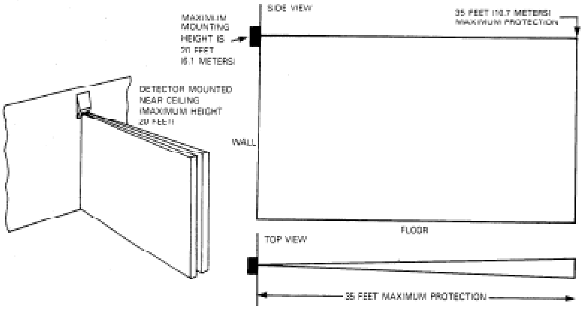
(DCNI) DCA LOCATIONS

DCA	Location
60	Topside Controlled Area (Exiting T5/V6)
59	Inside M1-M4 High and T4
61	Administrative Area (T4 High, T5 Low, D7, D12, D13, V5 to V6 Low, not beyond B7/B14/B15)
62	B7 Interlock
63	A-Side Maintenance Bay
64	A-Side Hallway
65	B14 Interlock
66	B-Side Maintenance Bay
67	B-Side Hallway
68	B-15 Interlock
69	B10 Mechanical Room
70	B11 Mechanical Room



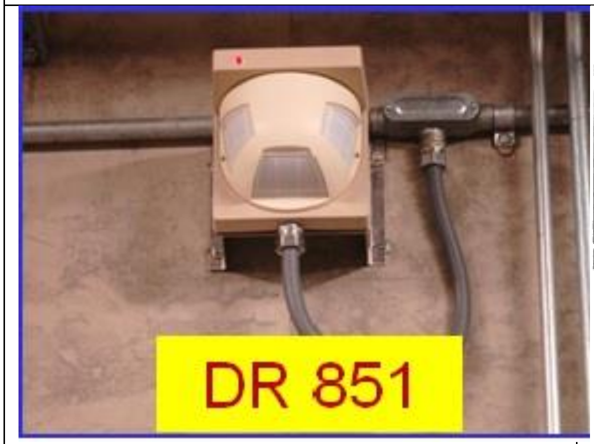
ATTACHMENT 5
(FOUO) IDS SENSORS




SIDE VIEW
MAXIMUM MOUNTING HEIGHT IS 20 FEET (6.1 METERS)
35 FEET (10.7 METERS) MAXIMUM PROTECTION
DETECTOR MOUNTED NEAR CEILING (MAXIMUM HEIGHT 20 FEET)
WALL
FLOOR
TOP VIEW
35 FEET MAXIMUM PROTECTION

DR301 Curtain Passive Infrared

Detection: Volumetric. Detects change in infrared energy emitted by objects entering the field of view.
Range: 35 feet.
Field of view: Curtain type.
Tamper: Yes, tamper switch located on the right side of the Hoffman enclosure.



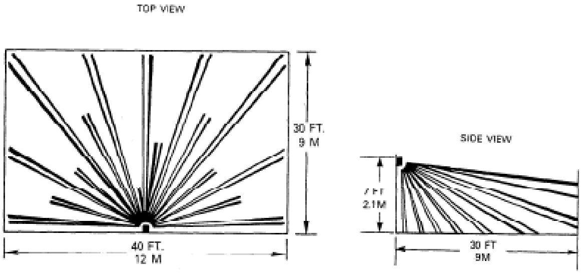
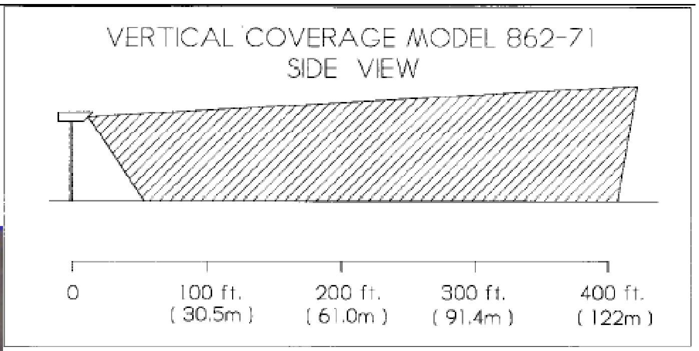
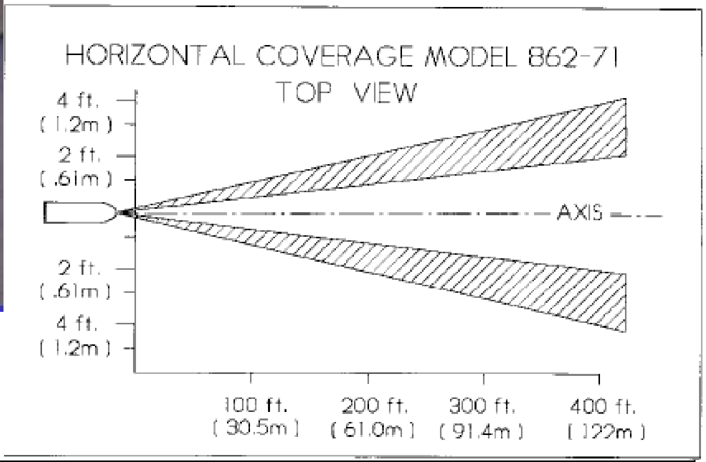


FIGURE 5-21. Passive Infrared Sensor DR-851, Detection Pattern

DR851 Area Passive Infrared

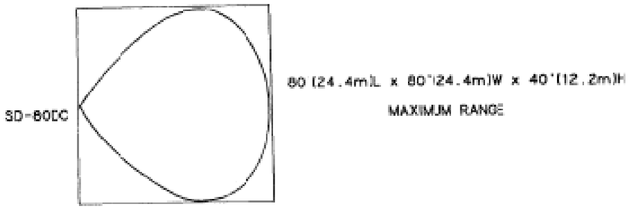
Detection: Volumetric. Detects change in infrared energy emitted by objects entering the field of view.
Range: 45 feet.
Field of view: 180 degree.
Tamper: Yes, microchip located inside.

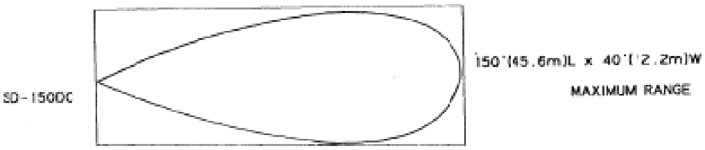




ELTEC 862-71 Telescopic Passive Infrared

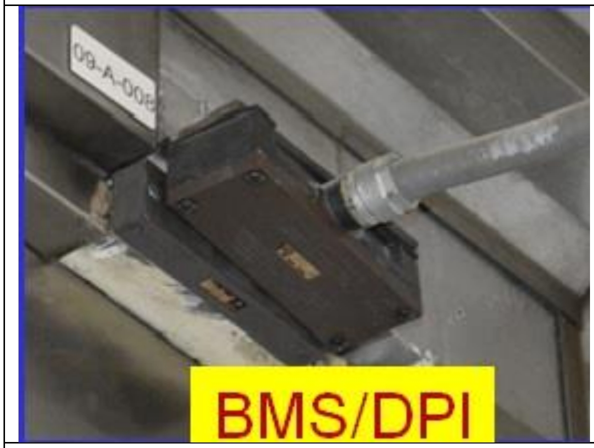
Detection: Volumetric. Detects change in infrared energy emitted by objects entering the field of view.
Range: 500 feet.
Field of view: Cone.
Tamper: Yes, microtamper chip located on the back.





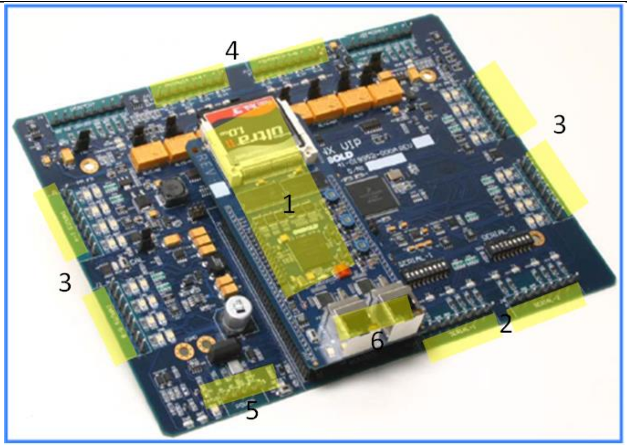
StereoDoppler 80/150 Microwave

Detection: Volumetric. Microwave energy detects movement.
Range: 80x80, 150x40
Field of view: Circle, Oval
Tamper: Yes, microtamper switch located on the inside.



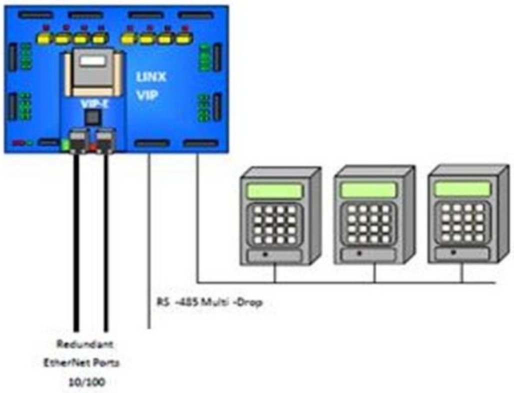
Sentrol 2087t Balanced Magnetic Switch/Door Position Indicator

Detection: Mechanical. Detects physical opening of doors, windows, and gates.
Range: Device will alarm upon separation of magnet (door) and reed switch (door frame).
Field of view: N/A.
Tamper: Yes, plunger tamper located inside reed switch.



1. VIP-E (Two 10/100MB ports (6)). Powered from the LINX VIP (Shown).
2. Serial ports; Can support 8 multi-drops per serial port.
3. Monitor ports; 1-16, 4 per port.
4. Relay ports; 1-8; 4 per port.
5. Power; left pin 1 and 2 A/C, pin 3 D/C, pin 4 GND.
6. 10/100MB communication ports. Left is primary, right is backup.

Multi-dropped Devices (Card Readers)



ATTACHMENT 6
SF OPERATIONAL TEST PROCEDURES

A6.1. _____ **Tamper Test.** Prior to CTS conducting maintenance, SSCC will ensure all personnel present are listed on the maintenance authorization letter. Tests will be conducted in accordance with CTS workcards and ESS checklist.

A6.2. _____ Operator will ensure device and all associated alarms are secure.

A6.3. _____ Once verified secure, the CTS will open the device/door slowly, ensuring an alarm is received prior to an individual having the opportunity to gain access to the device.

A6.4. _____ If the alarm annunciates prior to an intruder being able to gain access, the test is successful, terminate testing. If the alarm does not annunciate prior to an intruder being able to gain access, the test is unsuccessful, follow the next step.

A6.5. _____ CTS personnel will adjust the device as needed to ensure compliance. Once adjustments have been made the test will be re-accomplished.

A6.6. _____ **Intrusion Test (BMS).** Operator will ensure device and all associated alarms are secure.

A6.7. _____ Once verified secure the door/window associated with the sensor will be slowly opened, ensuring an alarm is received prior to an individual having the opportunity to gain access to the resource. Follow steps A6.4 to A6.5.

A6.8. _____ **Intrusion Test (PIR/Microwave).** Operator will ensure device and all associated alarms are secure.

A6.9. _____ Once verified secure an individual will make three (3) attempts at one-foot per second to penetrate the field of coverage from all likely avenues of approach. Follow steps A6.4 to A6.5.

A6.10. _____ **Workstation Operational Test.** Utilize QRC D16 and conduct a Routine Verification.

ATTACHMENT 7
AFTO 781A PROCEDURES

A7.1. _____ FROM – Indicates the date the JCN was opened in YYYYMMDD format.

A7.2. _____ TO – Indicates the date the JCN was closed in YYYYMMDD format.

A7.3. _____ PAGE OF PAGES – Indicates number of pages associated with the AFTO Form 781a.

A7.4. _____ SYM – Indicates priority level of JCN in 1/2/3 format.

A7.5. _____ JCN – Indicates the Job Control Number received by MC in YY-JJ-NNNN format. JJ indicates Julian calendar date and NNNN indicates the work order number.

A7.6. _____ DATE DISC – Indicates the date the discrepancy was discovered in YYYYMMDD format.

A7.7. _____ DATE CORRECTED – Date the discrepancy was corrected in YYYYMMDD format.

A7.8. _____ DISCREPANCY – Description of discrepancy associated with device with three lines; time/discrepancy, compensatory measures, and CTS response.

A7.8.1. _____ Time/Discrepancy – DD Mon YYYY @ TTTT: Device, discrepancy. E.g., 16 Oct 2014 @ 2200: 2/24 B1 High Card Reader Tamper

A7.8.2. _____ Compensatory measures – Operator types “Compensatory Measures:” and indicate the type of compensatory measure required, if required.

A7.8.3. _____ CTS Response – Operator types “DD MMM YYYY @ TTTT CTS on scene:” and indicates the two authorized maintenance personnel that responded.

A7.9. _____ DISCOVERED BY – Indicates the alarm monitor on duty when discrepancy discovered in “Rank Last Name, First Name MI.” format.

A7.10. _____ EMPLOYEE NO. – Indicates duty section.

A7.11. _____ CORRECTIVE ACTION – Description of corrective actions taken by ESS maintenance personnel. Any updates will be indicated in a “DD MMM YYYY @ TTTT:” format with Rank/Name of two authorized maintenance personnel that responded.

A7.11.1. _____ Operational tests – Indicates required operational test conducted after finishing maintenance/repairing discrepancy.

A7.11.2. _____ CORRECTED BY – Indicates the two authorized maintenance personnel that conducted troubleshooting/maintenance on discrepancy.

A7.11.3. _____ INSPECTED BY - Indicates the alarm monitor on duty when discrepancy discovered in "Rank Last Name, First Name MI." format.

A7.11.4. Blotter entry will be conducted by the SCS.

ATTACHMENT 8
(FOUO) IDS COMPENSATORY MEASURES

DISCREPANCY	DEVICE/LOCATION	COMPENSATORY MEASURE
SENSOR FAILURE	Controlled Area	4 hour checks
SENSOR FAILURE	Limited Area	1 hour checks
SENSOR FAILURE	2-Person Area	30 minute CCTV checks
SENSOR FAILURE	B5/B6 escape hatch PIR	4 hour checks
TAMPER	Field Distribution Box	
	Controlled/Limited Area	30 minute checks
	2-Person Area	30 minute CCTV checks
TAMPER	Junction Box	
	Controlled Area	1 check per shift
	Limited Area	1 hour checks
	2-Person Area	30 minute CCTV checks
TAMPER	Console	2 hour checks; ISRT notifies RDAO (if ECP) or Remote (if SSCC/MC)
TAMPER/LINE FAULT	BMS, PIR, Microwave	
	Controlled Area	4 hour checks
	Limited Area	1 hour checks
	2-Person Area	30 minute CCTV checks
	B5/B6 escape hatch PIR	30 minute checks
	Duress	Duress operational, no comp measure. Duress not operational, 30 minute status checks
TAMPER	Door Position Indicator	
	Limited Area	1 per shift
	2-Person Area	2 CCTV checks per shift
	DPI INOP	4 hour checks
TAMPER	Card Reader	
	Limited Area	1 hour checks
	2-Person Area	30 minute CCTV checks
TAMPER	Intercom	
	Limited Area	1 hour checks
	2-Person Area	30 minute CCTV checks
TAMPER	Booth	Lockdown booth
TAMPER	V2/V8, V1AA/V1AB Control Box	1 hour checks
COMM LOSS	Controlled Area VIP-E	No restore/assess affected

		areas/IDS, implement compensatory measures on affected IDS; Restore/assess affected areas/IDS
COMM LOSS	Limited Area VIP-E	No restore/Topside 360, assess affected areas/IDS, implement compensatory measures on affected IDS; Restore/assess affected areas/IDS
COMM LOSS	2-Person Area VIP-E	No restore/Topside 360, assess affected areas/IDS, implement compensatory measures on affected IDS; Restore/assess affected areas/IDS
COMM LOSS	Host VIP	Contact ESS NCO
COMM LOSS	Card Reader MUX	No Restore/assess affected MUX, contact ESS NCO; Restore/assess affected MUX
WORKSTATION	LDAO FAILURE	RDAO assumes primary control of workstation, post additional SCAM/SCS in SSCC
WORKSTATION	RDAO FAILURE	Post additional certified SEC at ECP
POWER	A/C FAIL, no restore	Contact ESS NCO
POWER	LOW BATTERY	Contact ESS NCO
WSTI/LRTI	Video Loss	N/A
	Tamper	4 hour checks
CCTV	Video Loss	When opening/closing doors ensure a patrol has visual of personnel and equipment and relays everything is all clear before opening/closing
	Tamper	4 hour checks

(All Comp measures that are in place will be annotated in the blotter)

ATTACHMENT 9
(FOUO) MAINTENANCE RESPONSE TIMES

EQUIPMENT MALFUNCTION	**PRIORITY 1** *(1 HOUR)*	**PRIORITY 2** *(24 HOURS)*	**PRIORITY 3** *(NEXT DUTY DAY NOT TO EXCEED 72 HOURS)*
TWO-PERSON AREA SENSOR	X		
LIMITED AREA SENSOR		X	
CONTROLLED AREA SENSOR			X
TWO-PERSON AREA SENSOR TAMPER/LINE FAULT	X		
LIMITED AREA SENSOR TAMPER/LINE FAULT		X	
CONTROLLED AREA SENSOR TAMPER/LINE FAULT			X
EQUIPMENT ENCLOSURE TAMPER (WORKSTATIONS, FDB, BPS, BOOTH, CARD READER, JBOX)		X	
ANNUNCIATOR EQUIPMENT	X		
PRIMARY/BACKUP COMM LOSS WITH RESTORE			X
PRIMARY/BACKUP COMM LOSS NO RESTORE	X		
AECS ENROLLMENT SYSTEM FAILURE	X		
AECS PORTAL FAILURE			X
AECS BOOTH FAILURE (If 1-3 booths are INOP)			X
AECS BOOTH FAILURE (If all booths are INOP)	X		
RTES FAILURES RENDERING ALL WEAPONS INOP	X		
INOP BMS ON RTES			X

TOWER DOOR			
ADJUSTMENTS TO CLAMSHELLS THAT AFFECT SAFE OPERATION OR ENVIRONMENTAL INTEGRITY OF WEAPONS SYSTEM	X		
PERIMETER SURVEILANCE RADAR SYSTEM FAILURE			X
WIDE AREA SURVEILANCE THERMAL IMAGER FAILURE			X
LONG RANGE SURVEILANCE THERMAL IMAGER			X
CCTV FAILURE			X

ATTACHMENT 10
(FOUO) SPECIAL FUNCTIONS AND INTERLOCK LOGIC

ECP Special Functions			
To Open	**Secure**	**Open**	**Security Posting**
Mini EC-1	V5/V6/V7/V8, EC2, MC2/MMALL/SCS1	V2/V3/V4	Patrol at V2
EC-1	V6/V7/V8, B1/B2, EC2, MC2/MMALL/SCS1	V2/V3/V4/V5	Patrol at V2
EC-2	V2/V3/V4/V5, B1/B2, Mini-EC1/EC1, MC2/MMALL/ SCS-1	V6/V7/V8	Patrol at V8
EC-ALL	B1/B2	V2/V3/V4/V5/V/V7/V8	Patrol at V2 and V8

SSCC Special Functions			
To Open	**Secure**	**Open**	**Security Posting**
MC-2	B1/B3/B5/B6/B7/B8/B9/B10/B11/B12/B13/B14/B15, V2/V5/V6/V8, EC1/EC2/Mini-EC1/ECALL, MM7/MM9/MM12/MM14/MM-ALL/SCS1	B2/B4	ISRTs in Brandt Hall
MM-7	B1/B2/B3/B4/B5/B6/B9/B10/B11/B12/B13/B14/B15, MM9/MM12/MM14/MC2	B7/B8	ISRTs in Brandt Hall
MM-9	B7, MC2/MM7/MM14/SCS1	B8/B9	N/A
MM-12	B14, MC2/MM7/MM14/SCS1	B12/B13	N/A
MM-14	B1/B2/B3/B4/B5/B6/B9/B10/B11/B12/B15, MC2/MM7/MM9/MM12/SCS1	B13/B14	ISRTs in Brandt Hall
MM-All	B1/B2/B3/B4/B5/B6/B10/B11/B15, EC1/EC2/Mini-EC1/EC-ALL, MC2/SCS1	B7/B8/B9/B12/B13/B14	ISRTs in Brandt Hall
SCS-1	This function closes all blast doors and vehicle gates in the facility regardless of interlock configuration.	N/A	ISRTs in Brandt Hall

Vehicle Barrier/Gate/Door Interlock Logic Combinations		
To Open	**Secure**	**Security Posting**
V2	V3, EC2, MC2/SCS1	Patrol at V2
V3	V2/V4, EC2, SCS1	N/A
V4	V3/V5, EC2	N/A
V5	V4/V6, Mini-EC1/EC2, MC2	N/A
V6	V5/V7/V8, Mini-EC1, EC1	N/A
V7	V6/V8, Mini-EC1/EC1	N/A
V8	V6/V7, Mini-EC1/EC1, MC2	Patrol at V8

Blast Door Interlock Logic Combinations	
To Open	**Secure**
B1	B3/B4, EC1/EC2/ECAll, MC2/MM7/MM14/MMAll/SCS1
B2	B3/B4, EC1/EC2/ECAll, MC2/MM7/MM14/MMAll/SCS1
B3	B1/B2, MC2/MM7/MM14/MMAll/SCS1
B4	B1/B2, MC2/MM7/MM14/MMAll/SCS1
B5/B6	MC2/MM7/MM14/MMAll/SCS1
B7	B8/B9, MC2/MM9/MM14/SCS1
B8	B7/B9, MC2/MM14/SCS1
B9	B7/B8, MC2/MM7/MM14/SCS1
B10	B11/B15, MC2/MM7/MM14/MMALL/SCS1
B11	B10/B15, MC2/MM7/MM14/MMALL/SCS1
B12	B13/B14, MC2/MM7/MM14/MMALL/SCS1
B13	B12/B14, MC2/MM7/SCS1
B14	B12/B13, MC2/MM7/MM12/SCS1,
B15	B10/B11, MC2/MM7/MM14/MMALL/SCS1

NOTE: The Terrorist Push Button located on the SCS console, when activated, will cut off the hydraulics to B1-4. B1/3 will still have the ability to be opened using AECS.

ATTACHMENT 11
X-RAY TESTING

A11.1. _____ Inbound and Outbound X-ray will be tested prior to shift change relief.

A11.2. _____ Inspect the test kit and all contents for signs of damage.

A11.3. _____ Place the test kit on the X-ray.

A11.4. _____ Run the X-ray forward until a full image of the test kit displays on the X-ray monitor.

A11.5. _____ Ensure the image is clear on both the B/W and color monitors.

A11.6. _____ Test the zoom-in and zoom-out functions.

A11.7. _____ Test each feature of the X-ray using the photographic examples in the X-ray test book.

A11.8. ___ If the X-ray test fails, initiate a P2 JCN.

Status	X-ray Feature
	Normal Black and White
	B/W Reverse
	B/W Pseudo
	Edge Tracing
	High-Pen
	Normal Color
	Color Inorganic Stripping
	Color Organic Stripping
	Color Edge Tracing
	Color High-Pen

Black and White		
Test Piece	**Represents**	**Color**
Metal Scale	Metal Thickness	Dark with viewable strip
Wire Scale	Wiring Devices	#25 wire visible
Thin Metal	Contact Switches	Dark
Copper	Copper Conduit	Light Gray
Salt	Inorganic Material	Light Gray
Sugar	Organic Material	Light Gray

Black and White Reverse		
Test Piece	**Represents**	**Color**
Metal Scale	Metal Thickness	White
Wire Scale	Wiring Devices	Black to gray shaded
Thin Metal	Contact Switches	Dark Gray
Copper	Copper Conduit	Light Gray
Salt	Inorganic Material	Light Gray
Sugar	Organic Material	Light Gray

Black and White Pseudo		
Test Piece	**Represents**	**Color**
Metal Scale	Metal Thickness	Black
Wire Scale	Wiring Devices	Violet to Dark Purple
Thin Metal	Contact Switches	Grey to Green
Copper	Copper Conduit	Red-Brown
Salt	Inorganic Material	Dark Purple
Sugar	Organic Material	Light Purple

Black and White Edge Tracing		
Test Piece	**Represents**	**Color**
Metal Scale	Metal Thickness	Lightly Outlined
Wire Scale	Wiring Devices	Lightly Outlined
Thin Metal	Contact Switches	Lightly Outlined
Copper	Copper Conduit	Lightly Outlined
Salt	Inorganic Material	Lightly Outlined
Sugar	Organic Material	Lightly Outlined

Black and White Hi-Pen		
Test Piece	Metal Thickness	**Color**
Metal Scale	Wiring Devices	Lightly Outlined
Wire Scale	Contact Switches	Gradual Gray-scale
Thin Metal	Copper Conduit	Lightly Outlined
Copper	Inorganic Material	Lightly Outlined
Salt	Organic Material	Dark Grey
Sugar	Metal Thickness	Light Grey
Color		
Test Piece	**Represents**	**Color**

Metal Scale	Metal Thickness	Black, Green, and Blue
Wire Scale	Wiring Devices	Dark to Light Green
Thin Metal	Contact Switches	Light Green
Copper	Copper Conduit	Dark Blue
Salt	Inorganic Material	Green
Sugar	Organic Material	Orange

Color Organic Stripping		
Test Piece	**Represents**	**Color**
Metal Scale	Metal Thickness	Teal to Brown
Wire Scale	Wiring Devices	Gradients of Brown
Thin Metal	Contact Switches	Light Grey
Copper	Copper Conduit	Dark Grey
Salt	Inorganic Material	Grey
Sugar	Organic Material	Orange

Color Inorganic Stripping		
Test Piece	**Represents**	**Color**
Metal Scale	Metal Thickness	Silver to Blue
Wire Scale	Wiring Devices	Blue to Light Blue
Thin Metal	Contact Switches	Light Blue
Copper	Copper Conduit	Dark Blue
Salt	Inorganic Material	Blue
Sugar	Organic Material	Grey-Blue

Color Edge Trace		
Test Piece	**Represents**	**Color**
Metal Scale	Metal Thickness	Lightly Outlined
Wire Scale	Wiring Devices	Lightly Outlined
Thin Metal	Contact Switches	Lightly Outlined
Copper	Copper Conduit	Lightly Outlined
Salt	Inorganic Material	Lightly Outlined
Sugar	Organic Material	Lightly Outlined

Color Hi-Pen		
Test Piece	**Represents**	**Color**
Metal Scale	Metal Thickness	Solid Black
Wire Scale	Wiring Devices	Dark Green to Light Green
Thin Metal	Contact Switches	Green to Light Green
Copper	Copper Conduit	Dark Blue
Salt	Inorganic Material	Green
Sugar	Organic Material	Orange

ATTACHMENT 12
METAL DETECTOR TESTING

A12.1. _____ Pass test piece through the lower portion of the metal detector. If an audible and visual alarm annunciates, proceed to the next step.

A12.2. _____ Pass the test piece through the middle portion of the metal detector. If an audible and visual alarm annunciates, proceed to the next step.

A12.3. _____ Pass the test piece through the upper portion of the metal detector. If an audible and visual alarm annunciates, terminate the test.

A12.4. ____ If any step fails (no audible and visual alarm annunciation), initiate a P2 JCN.