Fort Hood Alarm Monitoring Station
Government Standard Operating Procedures
May 2025

Table of Contents

Applicability, page 4

General information, page 4

Restricted area, page 4

References, page 4

Contact numbers, page 5

Incoming shift, page 6

Outgoing shift, page 6

Self-identification, page 6

Workspace, page 6

Breaks, page 6

Shift event logs, page 6

Daily reporting, page 6

Service requests for IDS during normal business hours, page 7

Service calls for IDS outside normal business hours, page 7

Catastrophic failures, page 7

Scheduled power or network outages 7

Suspected power outages, page 7

Suspected network outages, page 8

Posting of guards, page 8

Unaccompanied access rosters (UAR), page 8

Unaccompanied access rosters known issues, page 9

Notifications, page 9

Periods of IDS failure notifications 9

Restoration of IDS failure notifications, page 10

IDS priority levels, page 10

Documentation reminder, page 10

IDS components, page 10

Device status reporting, reported alarm types and states, alarm definitions, page 10

Alarm response time, page 10

Cancelling a call, page 11

Alarm acknowledgement, page 11

Adding notes and resolution codes, page 11

Clearing procedures, page 11

APC UPS AC power fail, page 11

ACP UPS low battery, page 12

AC power fail, page 12

Low battery, page 12

Network enclosure tamper, page 12

Keypad violation, page 12

Breached, page 12

Bad seal, page 13

Duress, page 13

Radio frequency (RF) duress, page13

Duress self-reset, page 13

Duress tamper, page 13

Duress reset keys, page 14

General Officer Quarters (GOQ), page 14

Command Suite Duress, page 14

Intrusion alarm HSS or combination HSS and PIMS, page 14

Tamper alarm cabinet, HSS or PIMS, page 15

Intrusion PIMS, page 15

Intrusion HSS, page 15

HSS 24/7 protection alarms, page 15

Points with no sensor assignment (Spare Point), Page 16

Shunt, page 16

Remote access and secure, page 16

SCIF alarms, page 16

SCIF shunting, page 16

Timed response test, page 17

Zone testing, page 17

Appendix A – Abbreviations and Definitions, page 18

Appendix B – AMS Facility Access Roster, page 20

Appendix C – DES Law Enforcement SOP (IDS extract), page 21

Appendix D – Fire/Evacuation Procedures 27

Appendix E – Building 23020 Evacuation Map, page 29

Appendix F – Command Emergency Entrance Procedures (CEEP), Page 30

Applicability: Any person performing Alarm Monitoring duties at the Directorate of Emergency Services (DES) Alarm Monitoring Station (AMS).

General Information: The Intrusion Detection System (IDS) at Fort Hood is the Integrated Commercial Intrusion Detection System (ICIDS) managed by the Directorate of Emergency Services (DES). The ICIDS manages IDS, Entry Control Equipment (ECE), and Closed-Circuit Television (CCTV). The current ICIDS system is configured to manage both IDS and ECE. The Alarm Monitor shall use alarm resolution procedures for various types of alarms as described throughout this SOP. Both electronic and telephonic correspondence shall be made with various other Government agencies on Fort Hood during normal business hours and after-duty hours.

This SOP does not address every situation that could arise; however, serves as a guide to address the most common situations that will be applicable to other possible scenarios. This SOP is a living document and adjusted as necessary to provide the most current guidance.

Restricted Area: The Alarm Monitoring Station is a restricted area, only authorized personnel are allowed access to the AMS located in building 23020, room 112. The Contracting Officer's Representative (COR) shall provide updated access rosters to the AMS personnel as changes occur. Requests for access by personnel not on the access shall be advised to contact the COR. If the COR is not able to be reached, the alarm monitoring person on duty shall refer to the authorized access roster to contact an authorized Government Representative and request an escort for the visitor.

References: The AMS operator shall be responsible for maintaining all required regulatory and non-regulatory guidance in the AMS Area. Recommended way of maintaining is downloading from the Army Publishing Directorate http://www.apd.army.mil/. The below listed shall be stored in the public documents folder on the Government provided computer workstation for quick reference. The COR shall provide initial listed regulations for inclusion into the shared folder. The AMS operators shall receive the PWS from their lead/supervisor.

- Contract Performance Work Statement (PWS).
- AR 190-11, Physical Security of Arms, Ammunition, and Explosives.
- AR 190-13, The Army Physical Security Program.
- AR 190-51, Security of Unclassified Army Property.
- CDRL A023, ICIDS-V System User Training Guide.

Contact Numbers:

Alarm Response Request:

Police Dispatch Center	288-1024	287-7127
Military Police Desk (Station Operations)	287-4001	

Alarm Monitoring Station:

Alarm monitoring	287-7703	288-0872

Directorate of Emergency Services:

Contracting Officer's Representative (COR) ***(cell number not for public release*)**	(o) 287-4966 *(cell) 254-913-8992*
Alternate COR ***(cell number not for public release)***	(o) 287-5035 *(cell) 254-392-5765*
Personal Identification Number (PIN) Office	287-1934
Chief, Access Control	287-3508
Chief, Physical Security Branch	287-4900
Physical Security Team Lead (Blue Team)	287-3535
Physical Security Team Lead (Red Team)	287-1731
Physical Security Specialist	287-4915
Physical Security Specialist	287-4974
Physical Security Specialist	287-4463
Physical Security Specialist	287-1943
Physical Security Specialist	287-1923
Physical Security Specialist	287-3818
Physical Security Specialist	287-5035
DES Operations	287-3613
Information Technology (DES computer support)	287-8019
Information Technology (DES computer support)	553-3294

Government Agency Numbers:

Department of Public Works (DPW)	287-2113
Network Enterprise Center (NEC) Operations ***Duty hours***	287-1530
Army Enterprise Service Desk ***(for customers during duty hours)***	1-866-335-2769
Network Enterprise Center ***After hours***	254-360-6782
Fort Hood Installation Operations Center (IOC)	287-4963
Fort Hood Installation Operations Center (IOC)	287-2054
Fort Hood Installation Operations Center (IOC)	287-2520
III Corps (Building 1001) Site Security	288-6846
Neighborhood Community Center	285-2251

IDS Maintenance Support:

Maintenance Technician	
Maintenance Supervisor	

Incoming Shift: Review prior shift event logs for any ongoing alarm activity that will carry on to your shift. Receive briefing of any active alarm events from the outgoing shift. Ensure the prior person on shift has logged out of the Government computer and the StarWatch Security Monitoring Software (SMS) and log in to your own designated user account. If the prior person on shift fails to log off, log them off and log into your accounts.

Outgoing Shift: Ensure your shift event log is closed out and digitally signed before departing and log out of both the Government computer and the StarWatch SMS. Brief incoming shift of any issues and ongoing events that will carry on to the next shift.

Self-identification: When answering the phone, you shall always identify yourself by name, the office (alarm monitoring) and the contracted company you work for. There shall be no indications that you are a Government employee or active-duty soldier. Your email signature block shall also identify yourself by name, position (alarm monitoring), and the Contracted company you represent.

Workspace: Each shift shall ensure the workspace is always maintained in a high state of cleanliness. The counter work area should be maintained with a professional appearance, clean and free of clutter and unnecessary material.

Breaks: Meals and beverages shall be consumed within the alarm monitoring station, however, kept away from the immediate workspace near computers or their peripherals.

Shift Event Logs: All alarm monitoring personnel shall maintain a Shift Event Log during their tour of duty. The shift event log shall be used to record all pertinent information during the AMS operators' shift and shall be completed using the Government's computer. Each shift event log shall cover a 24-hour period beginning at 0001 and ending at 2400 for each day (24-hour period). Remember! All information noteworthy of being entered into the shift event log shall include who, what, where, why, and when. This shall include the name of the dispatcher taking the request for law enforcement and the name of the responding patrol. There is never too much information to provide. The rule of thumb is to ensure all information from the point of an alarm or situation occurs through to the point of resolution is document so that a 3rd person can look at the sequence of events and know the story. All phone numbers and names of personnel involved shall be included. In the event there is an instance of issues with the Government computer to electronically generate the logs; they shall be handwritten and transferred to electronic form when computer access is restored. The COR shall be notified that this scenario occurred and will be granted extended time to send the logs as identified in the daily reporting section of this SOP.

Daily Reporting: Pursuant to PWS part 5.5. The contractor shall submit the shift event logs (TE – B) to the Contracting Officer's designated representative via e-mail no later than 0900 hours each day, Monday through Friday. Monday reports will include events from Friday, Saturday and Sunday. The shift event logs will cover a 24-hour period beginning at 0001 and ending at 2400 for each day. This will result in a monitor generating more than one (1) log during a 24-

hour period since his/her last shift. The contractor shall also ensure that a copy of each shift event log is maintained on the government computer.

Service Requests for IDS During Normal Business Hours: Monday through Friday (including training holidays), when an IDS system is in failure the COR and alternate shall be notified by email and phone no later than 1 hour if the system is not restored.
Exception: when the failure occurs between 3:00 pm and 4:00 pm; the COR and alternate should be notified immediately. This allows ample time for the CORs to assess and have a technician repair if needed before close of normal business hours. All email notifications shall include the contracted maintenance contractor (email will be provided) to ensure they are aware of the situation in event the CORs are not immediately available. The goal is to minimize the posting of guards when a situation can be resolved during normal business hours.

Service Requests for IDS Outside Normal Business hours: Request for repair shall meet the criteria of a catastrophic failure and any single priority 1 or 2. The COR shall be notified using the after-hour cell phone number or the alternate COR if the primary is not available. Always leave a voice message when direct contact is not made with a brief description of the situation.

Catastrophic Failures: Catastrophic failures can occur for various reasons or for a combination of reasons such as severe weather, power, communications, major IDS component failure or damage by construction. The criteria for catastrophic failures are when 10 or more zones of any combinations of priority 1 through 6 go into failure *(see priority level table in this SOP).* This will require notification to the COR and/or his alternate as outlined in the above for normal business hours or outside normal business hours. The following shall occur in the event of an unscheduled catastrophic IDS failure occurring:

- AMS will notify the Directorate of Emergency Service (DES) military police desk (Station Operations). A list of impacted units will be provided as well. The MP Desk personnel will then notify the Installation Operations Center (IOC) of the outage and will provide the IOC with the list provided by AMS.
- AMS will make necessary notifications to the impacted units.
- Once IDS has restored, the AMS will notify the impacted units and the MP desk. The MP desk will then update the IOC.

Scheduled Power or Network Outages: The CORs are normally informed in advance of scheduled outages and will forward the information to the AMS personnel via email or calendar invite.

Suspected Power Outages: Power outages can impact a single facility or multiple. This could include power over a major networking facility. Typically, power failures impact more than 1 facility resulting in a catastrophic failure. Generally, you will see an AC power failure alarm(s) telling you power has been lost, and the system is running on backup battery. If the power is lost and another network device is impacted the zone can go into communications failure before the AC power failure alarm can come through. This can give a false interpretation, there is a network outage when the real problem resides with power. If it appears to be power related,

always contact the Department of Public Works (DPW) to inquire if they have any scheduled outages or

reports of unscheduled power outage. Their phone number list in the above *contacts table* has a 24/7 answering service. If no power losses have been reported, provide your contact information for a return call if they should learn afterwards there is one. When notifying the commanders of the IDS failure, request that they verify they have power to their facility and if not on site they need to go on site to assess the situation and report back. Provide the information to the CORs during normal business hours or outside normal business hours when the criteria for catastrophic failure have been met. Follow up with any new information.

Suspected Network Outage: Like a power outage a mass communications failure can occur and leave you uncertain if the issue is power or communications. Should you learn from DPW there is a power outage this is likely the culprit for the communications failure. When there are no known power outages you shall contact the NEC Operations during business hours to inquire of any known outages or advise of one that is suspected so they can check into it. When notifying the commanders of the IDS failure request, they verify they have network on other devices (computer) in the facility if they are not currently in the impacted facility. Provide the information to the CORs during normal business hours or outside normal business hours when the criteria for catastrophic failure have been met. Follow-up with any new information.

Note: There is an IDS network that may be the cause. If this cause is not a NEC related network issue, follow reporting guidance above for service requests. Sometime the IDS maintenance or CORs will have to verify the IDS is fully functional before we can request assistance from the NEC. When in doubt notify the CORs.

Posting of Guards: The standard arms room SOP for Fort Hood identified the requirement for posting of armed guards during periods of IDS failure. The alarm monitoring personnel shall never tell customers to post armed guards or to release their guards. Units and organizations shall be advised when their IDS has failed or is no longer in failure. During periods of failure the unit or organization shall be notified "*to follow their SOP and any governing regulations or policy during periods of no IDS protection*". When the IDS failure is corrected and stable, notification of the IDS returning to operational status shall be provided. Keep in mind the term IDS failure may or may not be the system itself but rather the installation's communications or electrical infrastructure supporting the IDS. Internally on your shift event logs, the notice to follow SOP for IDS failure shall still be notated as guard posted and guard released. Posting of armed guards for priority levels 2 and 4 is pursuant to Army Regulation 190-11. Our goal is to not tell the customer what to do and how to do it; but rather inform them to follow their SOP and any governing regulation for the asset being protected. Other priority levels such as SCIFs, open storage, and comsec should know what their requirements are during periods of no IDS.

Unaccompanied Access Rosters (UAR): The Personal Identification Code (PIC) office will update the electronic version of rosters prior to 4:00 pm each business day. At the end of each business day the person working in the PIC office will also bring updated hard copies. Should something not look updated during a business day contact the PIC office if any changes are

pending update in the electronic file and hard copy. If needed sooner than by 4:00 pm the PIC office can upload the electronic version upon request.

Unaccompanied Access Rosters Known Issues: UARs are generated and screened by both physical security and the PIC office be accepting. An unaccompanied access roster is a living document and the responsibility of a commander/supervisor or their appointed person to keep updated. In a perfect world they would do this, however it's very common for commanders or 1SGs to depart and the new commander does not update their assumption of command orders or the roster with their contact information. This can be learned when trying to reach a commander or 1SG or when a new one contacts AMS for information, but they are not on the roster or don't have assumption of command orders on file with us. Document the issue in the shift event logs and inform the new commander of the updates required to the PIC office. It is not the responsibility of the alarm monitoring personnel to determine the acceptable way a roster is populated. We strive to enforce all information that is populated, typed, digitally signed. Sometimes there are exceptions to this as determined by the CORs and physical security personnel during the screening of documents. It is possible to have handwritten changes, signatures, and other corrections as necessary to assist our customers in protecting their assets. When errors are found such as incorrect phone numbers, document in the shift event logs and notify the CORs and PIC office via email so we can obtain a corrected document.

Notifications: You will have access to both electronic unaccompanied access rosters accessible through the Government computer and by hard copy within the office space. For military organizations you will always begin the notification process with the commander. If the commander is unreachable leave a voice mail before contacting the First Seargent (1SG). if there is no contact with the 1SG, then you may begin contacting the primary armorer and alternate until someone is reached. If no one can be reached, and messages left, contact the Staff Duty Office (SDO). For civilian and SCIF rosters pay attention to the notification process as they may have a separate list on their roster for who to notify first. For commanders and supervisors, we must have Assumption of Command Orders on file to discuss the zone's status. Likewise, any person inquiring about the status of a zone must be on the unaccompanied access roster. See above for more information on unaccompanied access rosters.

Periods of IDS Failure Notifications: In most cases IDS protected areas have a governing army regulation and/or SOP for how the users will protect their assets during period of no IDS protection. The most common thing in Fort Hood is the posting of an Armed Guard (arms rooms) or occupancy by the appropriate cleared person (Open Storage or SCIF). In either case they are posting guards. When a zone has lost its IDS protection notify personnel (in sequence listed above) of the outage and to follow their SOP for periods of IDS protection. Provide any detail known e.g. power or network issue and/or known IDS component failure. Also, this is when you obtain information from them to help assist with obvious things such as power, or network related problems at a facility. When you submit your service request this information is helpful to the COR in determining who needs to be notified for further assistance. IDS failures are normally for short periods. Once the IDS failure has remained in continuous failure for 30 minutes, notifications shall begin. When the outage is scheduled or obvious in nature (such as power line/pole down, trenching damage), notifications shall be immediately once known.

Restoration of IDS Failure Notifications: Once IDS has restored to an operational status the general rule of thumb is to give the zone one (1) hour of stabilization before notifying the unit(s) the IDS is operational again. This prevents us from turning around and calling again if the system

did not stay up and failed again. This is the best practice when a zone is failing and restoring repeatedly. In some situations, notifications can be made immediately after an IDS technician, NEC, or DPW has made a repair.

IDS Priority Levels: IDS priority levels do not change the priority of how an alarmed zoned is responded to by alarm monitoring. All priority levels are treated the same as it pertains to your alarm resolution procedures. Only exception is when different alarms are received at the same approximate time, priority 1 SCIF zones will be responded to first. Different priority levels are primarily for the Government and alarm monitors to distinguish categories of the different zone types.

Priority 1	SCIFs
Priority 2	Bunkers, Explosives containers, and bulk weapons storage
Priority 3	General Officer and Command Suites
Priority 4	Unit AA&E Storage Facilities (Arms Room)
Priority 5	Open Storage, COMSEC, Museums, Utilities
Priority 6	Clinics, Pharmacies, Court Rooms, Finance, Cash Cage
Priority 7	DES Assets
Priority 8	Child Development Centers, most duress only zones
Priority 9	AAFES Facilities (PX) and DECA (Commissaries)
Priority 10	Non-Active alarm zone
No Priority Assigned	Access Control (Electronic Entry Control/Access Control Accounts)

Documentation Reminder: In all circumstances listed above and any following circumstances listed in this SOP, an accurate account of all alarmed event, failures, restorations, contacts incoming and outgoing will be documented in the daily shift event log.

IDS Components – Refer to CDRL A023, ICIDS-V System User Training Guide pages 13 – 30. In this section of the training guide, you will find photos of components, descriptions, and applications. Before proceeding further in your initial review of this SOP review and familiarize yourself with the components you are monitoring. If you need clarification of any system components and how they function consult with your supervisor or one of the CORs.

Device Status Reporting, Reported Alarm Types and States, Alarm Definitions: Refer to CDRL A023, ICIDS-V System User Training Guide pages 47 – 50. Before proceeding further in your initial review of this SOP review and familiarize yourself with the alarm status reporting, alarm types and alarm definitions you are monitoring.

Alarm Response Time: In most cases the IDS protected areas on Fort Hood have Army regulatory requirements for a police or security force response withing 15 minutes of an alarm

event. This means from the time the alarm is received, you request a patrol to respond, the patrol needs to be on site no later than 15 minutes after the alarm came into the StarWatch SMS console. Time is of the essence, do not delay in your decision-making process.

Cancelling a Call: Once a patrol has been requested you shall not call the dispatch center to cancel the call. Once a request is made let it play out through the process.

Alarm Acknowledgement: All alarms and status reporting will be acknowledged once it is received, and you begin your assessment for the appropriate alarm resolution procedures. No alarm will go unacknowledged no longer that 10 minutes. The StarWatch SMS stores every action taken in the system. During investigations where the event log shows no one acknowledged an alarm for hours later is unacceptable and reflects poorly of how you processed the alarm in a timely manner. For false or nuisance alarms that are reoccurring until resolved may be deferred by selecting the defer button however not until the initial alarm has been acknowledged first.

Adding Notes and Resolution Codes: When you acknowledge or clear the alarm, a window will pop up with the opportunity to add notes or select a resolution code e.g. false alarm, fault, genuine alarm, nuisance alarm, test, wind. Anytime additional information is available a note or resolution code shall be entered to the greatest extent possible. This allows a review of a single event in the server's database and have a permanent record of the event for investigative purposes or troubleshooting.

Clearing Procedures: Once the zone sensors are returned to a normal state and the responding patrol has provided all the necessary information of who, what, where, why, and when for entering in the shift event log; the alarm monitor may clear the alarm from the alarm queue. Always document the name of the responding patrol person and their patrol number. A patrol must clear the scene with alarm monitoring before the alarm can be cleared. In general, all alarm zones require a patrol to respond within 15 minutes of the alarm. If the patrol does not contact you withing another 15-20 minutes which should be enough time for them to investigate (30-35 minutes after initial alarm) you may need to contact dispatch and advise them you have not been contacted by the responding patrol.

APC UPS AC Power Fail: This alarm point is very frequent on Fort Hood due to degraded power infrastructure (referred to as dirty power). The APC UPS provides battery backup to the IDS network switch however does not support the NEC network switch and is sensitive with little fluctuation in a facilities power. Both switches are required to function for stable communications. While this is frequently a nuisance alarm due to recurrent states of alarming and returning to normal it will be closely monitored. If the APC UPS stays in failure for longer than 15 minutes, the unit will be notified and inquire if there are any known power related issues to the facility. If they do report a power issue, they shall be instructed to contact DPW to submit a work order. Notify the CORs of the failure with any additional information gathered from the

unit personnel during normal duty hours. This alarm point does not mean the IDS has failed however once batteries are depleted (typically 8-12 hours best case scenario) and power is not restored, the IDS will eventually fail. If the NEC switch *(98% of facilities the NEC switches do .not have battery backup or generators)* does not have battery backup or there is not a generator backup to the facility communications may be lost immediately.

APC UPS Low Battery: This alarm point usually occurs after an APC UPS AC Power Fail when power is lost for a short period and will go through a recharging process. This alarm will normally go back to normal however sometimes will be stuck and requires a technician to go on site to bring back into a normal mode.

AC Power Fail: unlike the APC UPS AC Power Fail this alarm point is not as common or as sensitive as the APC UPS. This alarm point is telling you the Remote Area Data Collector (RADC) has lost power. If the AC Power Fail stays in failure for longer than 15 minutes, the unit will be notified and inquire if there are any known power related issues to the facility. If they do report a power issue, they shall be instructed to contact DPW to submit a work order. Notify the CORs during duty hours of the failure with any additional information gathered from the unit personnel. This alarm point does not mean the IDS has failed however once batteries are depleted (typically 8-12 hours best case scenario) and power is not restored, the IDS will eventually fail. It is likely that you will also receive an APC UPS AC Power Fail with this AC Power Fail. Remember if the NEC network switch loses power too as mentioned above, the zone could go into immediate communications failure.

Low Battery: This alarm point means the RADC has a low battery. This can occur after an AC power fail and will recharge back to a normal state. Once the battery fails the system will go into communications failure.

Network Enclosure Tamper: This alarm point consists of 2 tamper switches on a cabinet door. All network enclosures have a sticker affixed identifying them as the property of the DES and have a contact number to the alarm monitoring station. Should someone call inquiring about the cabinet they shall be provided the COR's contact daytime number or to any number of a physical security inspector. If this point goes into alarm and stays in alarm this is a sign someone has opened the door. This requires a patrol to investigate the alarm. Notify the CORs during duty hours. Quite often these switches produce false alarms by rapidly alarming and resetting. Monitor to for several minutes to see if it stops. If stops, reoccurs, and stops again submit a service request. When in doubt, error on the side of caution and send a patrol.

Keypad Violation: This occurs when someone enters their PIC incorrectly. Most commonly this is seen with digital remote keypads. Only if the keypad violation results in an intrusion alarm shall you request a patrol to respond.

Breached: Most commonly this is a result of when a PIC holder does not exit the area within 30 seconds or re-enters the zone, motion detected resulting in an intrusion alarm. Other causes most common in a SCIF is a result of a tamper on the HSS 1 E/E. By design SCIF doors do not

have door closures to soften the closing of the door. The doors are heavier than a typical office door and when slammed tend to throw the HSS into tamper. To clear a breach a PIC holder

must “cycle the RADC”. This is completed by the PIC holder entering their PIC to either secure or access the zone and then enter their PIC again to either secure or access. A zone in breach will still send intrusion alarms if a person enters the zone. This does not require a guard

however to the best extent possible you shall attempt to get a PIC holder to cycle the RADC to clear the breach. The above examples are not all inclusive of a cause for a breach after the zone is secured.

Bad Seal: In the user guide the alarm definition is “Bad Seal” means the Zone was not armed correctly. We can mimic this alarm at during testing and means the person securing the zone did not get out in time before the 30 second countdown or re-entered the zone and left as the countdown completed but didn’t get back out before the 30 second countdown ended. If there is a bad seal and the mode is green secure, the zone is still protected, and alarms will be received if someone enters the zone. All assets are still protected. With this information, guidance if you receive a bad seal alarm do not request a patrol. Contact the person who secured as soon as possible to go back and access the zone then re-secure. A guard is not required.

Duress: *At no time will you contact the zone POC to inquire about the duress or to inform the duress is in alarm. The duress is a silent alarm, and the goal is to not alert the threat that law enforcement is responding.* Facilities with duress can have one or multiple duress. It is important when a facility has multiple duress to record the correct duress number (duress 1, duress 2,) in alarm and to inform the dispatch center of the specific duress number in alarm. All duress will be responded to regardless of the priority level including inactive zones (priority 10). All duress requires a key to reset except Radio Frequency (RF) duress. All responding patrols are provided with duress reset keys, physical security inspectors, and maintenance personnel.

Radio Frequency (RF) Duress: This device will have 2 buttons that must be pressed for 3 seconds to put it into an alarm state. When released it will restore to a normal state. Like all other alarm devices these will have a tamper alarm. These are wireless duress and will require the alarm monitor to remote access and secure again to clear the breach after a duress is triggered into an alarm state. The RF duress is limited to places such as select primary Access Control Points (ACPs), a general officer’s quarters, or a command suite duress. The RF devices will be identified on the zone map with the letters RF next the device widget.

Duress Self-Rest: All duress buttons are designed to lock in place and stay engaged (with exception to RF duress). The buttons at some locations are mounted under a desk or workspace and are invitations for a person to fidget with it by pushing the button but not fully engaging the duress to lock in an alarm mode. Most seen at ACP guard booths and administrative offices. Do not request a patrol for this nuisance or false alarm. Other causes can be cause by a faulty device. If reoccurring beyond several minutes, submit a service request.

Duress Tamper: Another common nuisance or false alarm when the device goes into tamper and self-resets. Common cause can be a chair or knee bumping into the device or objects being relocated in the room and bump into them. If reoccurring beyond several minutes, submit a

service request to the CORs with the maintenance contractor included. Do not request a patrol to respond. If the device goes into tamper and stays in a state of tamper request a patrol to respond. If the patrol finds no issue or evidence of tampering submit a service request.

Duress Reset Keys: As mentioned above all responding patrols should have a duress reset key on their vehicle's keychain. If a patrol over time has lost a key, they will have to request another patrol with a reset key to respond. They cannot be cleared until the duress is reset.

General Officer Quarters (GOQ): General Officer Quarters are equipped with duress within their living quarters. At no time shall there be attempts to contact the occupants. All contact with the occupants will be through the military police. The AMS operator shall notify the Police Dispatch Center of a communication failure at a General Officer's quarters. The military will investigate pursuant to their SOP (Appendix C). The AMS operator shall keep the Police Dispatch Center updated on the status of the alarm. For communications and power failures resulting in failure of the IDS; the police dispatch will be informed, and military police will follow their SOP.

Command Suite Duress: Command suite duress is in headquarter facilities within their senior leadership offices. These locations typically have no POCs for direct contact. Most command suite duress is equipped with RF duress. See above guidance for RF duress. Any tamper or communication failures do not require notification to unit personnel and do not need a request for a police or security office response. During normal duty hours contact one of the CORs and email a work order. The CORs will receive emailed work order requests when they return on the next duty day when issues occur outside normal business hours.

Intrusion alarm HSS or combination HSS and PIMS: When you receive intrusion alarms of HSS alone or a combination of HSS with PIMS alarms and the zone is not put into access within 30 seconds after alarm is received (total of 1 minute once the seal of the door is broken and not put into access before allotted 30 seconds to disarm expires) you shall:

- Look at the event log tab for the zone to see who was the last in the zone and/or most frequent person accessing and securing.
- Identify that person and make one (1) attempt to call the person to find out if the PIC holder is on site.
- If the PIC holder is on sight, advise the person he/she must disarm the zone immediately. Emphasize they have approximately 30 second to do so.
- If contact was made and the PIC holder ***does not*** disarm immediately as instructed and within 30 seconds, request for a patrol to respond.
- If the user is not on site immediately request a patrol to respond.
- If the PIC holder returns your call after a patrol was requested; advise the person a patrol is in route and to stand by for their arrival.
- When in doubt request a patrol.

Some locations you may be familiar with due to a person habitually forgetting to access the zone or slow to put in access. If you know a phone number inside the zone this can be the one (1) call to give the opportunity for them the put the zone in access. Same time limits as the above apply.

Tamper alarm Cabinet, HSS or PIMS: If the tamper alarm does not immediately restore while zone is in secure mode the sensors are not accessible. Contact the organization to inspect the area for signs of tampering with the sensors. Report a service request for maintenance technician. When a zone is in access mode follow the same guidance above for ***Intrusion alarm HSS or combination of HSS and PIMS.***

Intrusion PIMS: The Passive Infrared Motion Sensor (PIMS) detects motion. PIMS with an E/E next to it means the sensor is an entry/exit sensor. Sensors programmed as E/E are on a 30 second delay and will not alarm until 30 second if the zone is not put in access mode. A zone with multiple sensors may have more than 1 E/E PIMS if the PIMS will pick up motion at the primary entry exit door or HHS1 E/E. When the area is in secure mode with no breach of the HSS, possible causes for the alarm can be from motion triggered by the environment. Environmental causes are typically osculating fans, hanging objects from ceiling, printers, faxes, and rodents. These nuisance alarms are generally brief and will self-reset. Request the PIC holder to inspect the area for any environmental causes and signs of rodent dropping in the secure zone. This does not require a patrol to respond; however, if the motion is continuous or when the zone has multiple PIMS in alarm request a patrol and contact the commander to have an armorer meet the patrol to investigate. If nothing is found in either situation submit a service request.

Intrusion HSS: The High Security Switch (HSS) is a door contact that when in secure mode will detect if the door has been opened. The HSS with an E/E next to it means the sensor is an entry/exit sensor. Sensors programmed as E/E are on a 30 second delay and will not alarm until 30 second if the zone is not put in access mode. If there are other HHSs in a zone they will be programmed to instant intrusion. There will not be an allowable 30 seconds to enter or exit the area. Some arms rooms have issue windows that are protected by HSS. Issue windows will always be programmed to instant intrusion. Therefore, if the issue window is not properly closed it will prevent the armorer from properly securing the area. It is possible for an authorized PIC holder to open the vault door and not physically enter the zone which will cause an HSS alarm after 30 seconds if not disarmed and you receive no PIMS alarm. In any case a patrol shall be requested to respond. The HSS is most reasonable point of entry. The none “E/E” alarm does meet the criteria for a 1-time call attempt as outline in the above “*Intrusion alarm HSS or combination HSS and PIMS”.*

HSS 24/7 Protection alarms: Protection alarms are HSS sensors that are programmed to alarm 24/7 if a zone is in secure or access mode. This type of sensor is usually found on emergency egress doors within a SCIF or open storage space. Arms rooms will never have an emergency egress door. If you were not contacted by the site for notification they are using the door, request a patrol.

Points with no sensor assigned (Spare Point): Points with no sensor assigned are spare points. Meaning a technician can use it in place of a sensor point that fails or an additional sensor is needed in the zone. Typically, an alarm on a spare point result from a loose connection or a bad resistance reading. No action is required other submitting a work order. If a spare point is in alarm and keeping the zone from being secured or excessively going in alarm and normal it may be shunted until a technician can resolve the issue.

Shunt: Shunting is when a zone sensor is intentionally disabled. A sensor can only be put into shunt and taken out of shunt while the zone in in access mode. Shunting cannot be completed while the zone is secure. An alarm zone must always have two points of intrusion detection (HSS and PIMS). AMS shall never shunt a sensor when only these two points are protecting the asset. Unless there is more than one (1) PIMS a malfunctioning PIMS may be shunted until a

technician can repair to allow the PIC holder to secure a zone. An HSS regardless of quantity will never be shunted to allow a PIC holder to secure the zone. Duress switches may be shunted if it allows a PIC holder to secure the zone until a technician can resolve the issue. A malfunctioning sensor where a guard must be posted may be put into shunt until a technician repairs the sensor and the guard is released. Shunting may be temporarily long enough to cycle the RADC if a zone is in breach and the zone is occupied with personnel triggering motion alarms or opening doors. When a technician is on site making repairs always ask if he/she would like the shunt removed.

Remote Access and Secure: Using this feature will never be used on behalf of a PIC holder due to user error or to access or secure a zone due to malfunctioning sensors and to relieve the organization from increasing their own security posture during periods of no IDS. The only exception is with approval from the primary or alternate COR. Remote access and secure may be used to cycle the RADC to bring a system out of breach mode. Example may be a duress only zone or an inactive zone when there is no PIC holder. This feature may be used in an

inactive zone that has a tamper alarm or duress to determine if there if the motion sensor will detect someone actively in the area while a patrol responds.

SCIF Alarms: Sensitive Compartmented Information Facilities (SCIF) are the most secure facility with IDS protection and will receive the highest priority of response by the alarm monitor. SCIF zones are more complex than a standard IDS zone such as arms rooms. The SCIF has a Remote Status Monitor (RSM) that is identical to the Operator Workstation (OPWS) that the alarm monitors use. The SCIF personnel can monitor their alarms and activity internally, acknowledge, and clear alarms, and issue their own PICs for accessing and securing the zone.

As mentioned in the above *“Breached”* section and as another reminder*,* by design SCIF doors do not have door closures to soften the closing of the door. This ensures the door will close and lock. The doors are heavier than a typical office door and when slammed tend to throw the HSS into tamper. To clear a breach by tamper alarm, a PIC holder must “cycle the RADC”. This is completed by the PIC holder entering their PIC to either secure or access the zone and then enter their PIC again to either secure or access. These zones are normally highly populated so the chance of them clearing everyone out of the zone to cycle the RADC is unlikely and will not happen until the end of the business day when they secure for the night. Until this can be cleared, every time the door is opened and closed while the zone is in access will result in tamper alarm because the zone is in breach. Until the occupants can either cycle the RADC or secure the zone, you may defer the alarm until it can be cleared.

SCIF Shunting: Alarm points in a SCIF can only be shunted by a person with SCIF Remote Status Monitor (RSM) privileges. AMS personnel do not have any control of a SCIF zone

shunting or any other control such as remote access and secure. If you see a sensor within a SCIF go into shunt, no action is required.

Timed Response Test: SCIF personnel have a requirement to conduct a timed response test for a responding patrol or security force is on site within 15 minutes of an alarm. This testing is coordinated through the DES Operations office with the customer through a calendar invite email. The COR will forward the email to all alarm monitoring personnel to ensure they are aware of the coordinated test. Specific instructions will be within calendar invite.

Zone Testing: There a regulatory zone testing and maintenance requirements. The IDS maintenance personnel conduct maintenance and testing of each zone on a semi-annual basis, physical security inspectors every 18 months for an arms room and arms room armorers are required to perform system checks every month. SCIFs and Open Storage personnel must also test their zones however this schedule is sporadic depending on the persons managing the zones. Alarm monitoring shall assist all customers with the testing of their zones by acknowledging receipt of an alarm and restoration of the alarm produced by the tester, documenting the testing in the shift event log with the who, what, where, and why information including any devices that fail the test. A work order request shall be immediately submitted pursuant to the guidelines of this SOP. Requests from a customer to test the IDS shall not be declined unless real world circumstances are ongoing to a current alarmed event(s) which must take precedence. You can ask the customer to call back or obtain their contact information and offer to call back when there are no active real worlds events. Alternatively, the PIC office also conducts testing with customers and can be provided their contact number to see if their office can assist.

Appendix A
Abbreviations and Definitions

AAFES	Army Air Force Exchange System
AC	Alternating Current (power)
ACP	Access Control Point
AHA	Ammunition Holding Area
AMS	Alarm Monitor Station, Building 23020
AR	Army Regulation
AA&E	Arms, Ammunition & Explosives
CCTV	Closed Circuit Television
CDC	Child Development Center
CDRL	Contract Data Requirements List (User training guide)
CEEP	Command Emergency Entrance Procedures
Comsec	Communication Security
COR	Contracting Officer's Representative
DA Police	Department of the Army Police
DES	Directorate of Emergency Service
DPW	Directorate of Public Works
ECE	Entry Control Equipment
E/E	Entry/Exit
ESS	Electronic Security System
GOQ	General Officer Quarters
GSOP	Government Standard Operating Procedures
HSS	High Security Switch (also known as Balanced Magnetic Switch (BMS))
ICIDS-V	Integrated Commercial Intrusion Detection System-V (Current install alarm system at Fort Hood)
IDS	Intrusion Detection System
KO	Contracting Officer
MP	Military Police
NEC	Network Enterprise Center
NFC	North Fort Hood
OPWS	Operation Workstation
PIC	Personal Identification Code
PIMS	Passive Infrared Motion Sensor
PIN	Personal Identification Number
PMC	Primary Monitoring Console
POC	Point of Contact – Military or Civilian user's designated person(s) to contact.
PWS	Performance Work Statement
RADC	Remote Area Data Collector (IDS control panel)
RF	Radio Frequency (wireless device)
RSM	Remote Status Monitor
SCIF	Secured Compartmented Information Facility
SMS	Security Management Software
UAR	Unaccompanied Access Roster

UPS	Uninterruptable Power Supply
WFC	West Fort Hood
Zone	An IDS protected area

Appendix B
AMS Facility Activity Access Roster

Will provide at start of performance and updated throughout performance

Appendix C
Fort Hood Police Division SOP Section 2: Patrol Operations (18 March 2024)

a. General Officer Alarm. Army Regulation 190-13, *The Army Physical Security Program*, 27 June 2019, Chapters 9 and 10.

i. Patrol Response:

(a) The Station Commander will:

- Contact the Installation Operations Center (IOC), inform them of the alarm, verify if the General Officer (GO) is on or away from Fort Hood, and obtain the number for the GO / POC.
- Provide the information to the Watch Commander / Sector Supervisor by Computer Assistance Dispatch (CAD) or duty cellphone.
- Contact the GO quarters and ask to speak to the GO or one of his family members (FM). Script: **"Sir (or Ma'am), a Law Enforcement patrol has been dispatched to your quarters, please meet them outside and have your ID card in hand".** At no time will the GO or FM be informed that there is alarm activation. Should the GO or FM inquire, the Station Commander will repeat the statement.
- Make notifications IAW the Notification Matrix (See *Appendix C: Desk Operations*).
- Complete an SIR (Serious Incident Report) if required.

(b) The Watch Commander, Patrol Supervisor, or Sector Supervisor will:

- Move to the vicinity of the quarters (out of view from the quarters, if possible).
- Ensure the responding patrols establish TCPs to isolate the GO quarters at the intersections of (1) 24th Street at Sicily Drive, (2) Coleman Road and Patton Drive, (3) Sicily Drive and Normandy Court, and (4) Sicily Drive/Coleman Road/Todd Street.

- Make physical contact with the quarter's occupant(s) to determine if there is duress (Complete the GO Duress Alarm Inspection Sheet).

(i) IF NOT UNDER DURESS:

- The GO or FM will be asked to exit the quarters with their identification card and provide it to the Watch Commander, Patrol Supervisor, or Sector Supervisor who will complete the GO Duress Alarm Inspection Sheet.

- Upon verifying identification and no indication of duress, the Watch Commander or Sector Supervisor will ask if they can enter the quarters to verify there is no duress situation. Upon verification of no duress situation, all patrols may clear the scene. In the event the GO does not allow LE to enter the home for verification, telephonic notifications will be made to the Patrol Branch Chief and the Chief of Police.

(ii) IF UNDER DURESS:

- If the person indicates they are under duress, the person will be placed into the patrol vehicle and removed from the area. Upon removing the person to a safe area, the Watch Commander or Sector Supervisor will return to the quarter's area and contain the situation.

- The Watch Commander, Patrol Supervisor, or Sector Supervisor will maintain surveillance of the quarters.

- The Watch Commander will instruct the two patrols on scene to monitor egress routes from the quarters and to stop any suspicious vehicles/persons.

(c) The Patrol Officers will:

- Cordon off the area at the assigned TCP locations, position the vehicles so the in-car camera systems can capture all vehicles and pedestrians in the area.

- Take special instruction and guidance from the Watch Commander.

- Prepare a Police Report on all GO alarm (including false alarms).

Note: If under duress, establish an Incident Command Post to help control and manage the incident and contact the Military Police (MP) desk.

ii. Communications Alarm or Power Outage:

(a) The GO quarters response will initiate with a phone call to the resident/Aide de Camp, followed by a physical check of the quarters by the Watch Commander or Sector Supervisor.

(b) A patrol will monitor the area until the alarm system has been reestablished.

(c) During power outages, patrols conduct hourly checks of the quarters until the power is restored.

iii. Intrusion Alarm:

(a) The alarm monitor initiates Intrusion Alarm response with a phone call to the location, followed by a physical check of the location by the Watch Commander or Sector Supervisor. The Watch Commander will physically check the alarm, which is usually located in the personal office area or in the garage next to the electric breaker box.

(b) A patrol will monitor the area until the alarm system has been re- established.

(c) During power outages, patrols conduct hourly checks of the location until the power is restored.

iv. Points of Contact:

(a) Alarm Monitor Station: (254) 288-0872 or (254) 287-7703

(b) ESD: (254)-288-1024

(c) IOC: (254)-287-2054

v. III Armored Corps Headquarters Building Response:

(a) ESD will dispatch three patrols and the Watch Commander to BLDG 1001.

(b) Two patrols will establish a perimeter around the building via the east and west sides.

(c) The Watch Commander and a Sector Supervisor will go inside III Corps headquarters, make contact with the security guards, and verify the incident is valid.

(d) If the situation requires action, the Watch Commander will direct the patrols as necessary and establish an Incident Command Post (ICP).

b. Alarm Response (Bank/Business/SCIF/AA&E Storage). Task 191-389-0016, *Respond to an Alarm*

i. Procedures.

(a) ESD dispatches two patrols and specifies the location and type of alarm.

(b) If the alarm is called in by a third-party monitoring company, ensure the following information is included in the call card:

- Caller information
- Alarm type
- Location of alarm
- Incident or reference number
- Return POC information

(c) First Patrol Officer on scene places other patrols to ensure a 360-degree perimeter.

(d) Patrols should position themselves at a safe distance away from the facility. If a 360-degree view is not possible, patrols should be positioned to observe the main entry / exit points for the facility and traffic. Patrols will take cover behind vehicles and exercise appropriate officer safety and use of force procedures to ensure the safety all persons in the area.

(e) Patrols will not allow anyone other than LE personnel to enter the area. If anyone other than LE personnel attempts to leave the facility, the Patrol Officer should

order the person to halt and move them to a safe area.

(f) Patrols will request a contact number for a business supervisor at the location and call them. Patrols will then instruct the person to come outside the building and meet them. Ensure they describe what they are wearing and ensure positive ID. CAUTION: Persons exiting the facility may be suspects or released employees / hostages. Therefore, persons who exit the facility will be detained and not be allowed re-enter the facility.

(g) If the personnel exiting the facility have been identified as the Supervisor, NCO or officer who is verifying the status of the alarm, the person will be ordered to approach one Patrol while the other provides cover and maintains view of the building.

(h) Caution should be used at this time. If the patrol feels the person coming out is a threat, he should respond accordingly and order the individual into a safe position to be searched.

(i) The person will be ordered or escorted to a safe area and interviewed, if required.

NOTE: If any person flees, that person will not be pursued unless there is an adequate number of Patrols to maintain surveillance over the facility.

(j) Once positive ID is made with the Supervisor, Patrols escort the person back inside and check for any criminal activity.

(k) Once completed, AMS will be notified.

(l) Patrols will update the call card on their CAD or with dispatch with the person(s) they talked to and the outcome of the interview.

(m) IF FOUND UNSECURED AFTER BUSINESS HOURS:

- Patrol notifies dispatch, who contacts AMS to inactivate the alarms for the facility.

- Patrols will conduct a search of or around the facility for any person(s) and evidence of a crime.

- Once the patrol has completed the search:

(1) If negative finding, the patrol will contact AMS to obtain the POC to have the facility checked for damaged / missing property and secured.

(2) If the patrol cannot make contact with the POC or Building Manager and there are no signs of forced entry, patrols will conduct hourly checks and annotate the checks in their patrol reports.

(3) If the patrol discovers evidence of a crime, Patrols will contact the Watch Commander, MPI, and MWD to conduct a search for intruders and secure the scene. Refer to “Crime Scene Protection” of this SOP.

(n) Reports will be prepared on all alarms where facilities were found unsecured or there were signs of forced entry / criminal activity. False alarms will be recorded in the patrol reports, the journal, and the facility manager will be contacted.

ii. Phone Lines Down:

(a) ESD will dispatch one patrol to the alarm location.

(b) The patrol will contact the unit in charge of the facility.

(c) The patrol will instruct the unit to contact AMS and

post a guard until further notice.

(d) The patrol contacts AMS for further guidance.

(e) POINT OF CONTACT: AMS at (254) 288-0872 or 287-2762

Appendix D
Fire/Evacuation Procedures

Alarm Monitoring Station
Fire/Evacuation Procedures
Building 23020
Fort Hood, Texas 76544

1. All personnel employed by Alarm Monitoring Contractor and working at the Alarm Monitoring Station will be responsible knowing all Fire Plan and Evacuation procedures.

2. All signs of fire and/or smoke will be reported immediately to the Police Watch Commander.

3. AMS operators, upon assumption of duties, will check the AMS Fire Extinguisher to ensure it is properly charged and ready for use.

a. A 5 or 10 pound, AB or ABC, Fire Extinguisher is the only authorized Fire Extinguisher for the AMS Area.

b. A seal protecting the pin should not be broken and the gauge should show the needle in the green (Charged).

c. If there are any discrepancies with the Fire Extinguisher, they will immediately be reported to the Contract Program Manager and the Building Fire Marshal.

4. AMS operators use extreme caution when fighting any fire inside the AMS area, remember, there are electrical wires all around you, including under the floor.

5. If the AMS operator must evacuate due to excessive smoke and/or fire, follow the below listed procedures;

a. During duty hours, the AMS operator has only one way to exit the AMS area.

(1) Exit through the AMS Main Door

b. Depart building 23020 through the east door. If this route is blocked, depart the building through the west main entrance doors. (See Evacuation Map)

c. The AMS operator will then proceed to the designated rally point. This rally point is determined by the building Fire Marshal as a safe location for building personnel to assemble out of the way of responding emergency vehicles. This rally point will be indicated on the Evacuation Map.

d. Once the AMS operator is at the rally point, make contact with Police Desk personnel and brief them on the fire event (if any) in the AMS area, also make sure they understand that the AMS area was safely evacuated.

e. The AMS operator will then immediately notify the Contract Program Manager and the Contract COR.

f. The AMS operator will not return to the AMS area until it is cleared by the Fire and Police authorities.

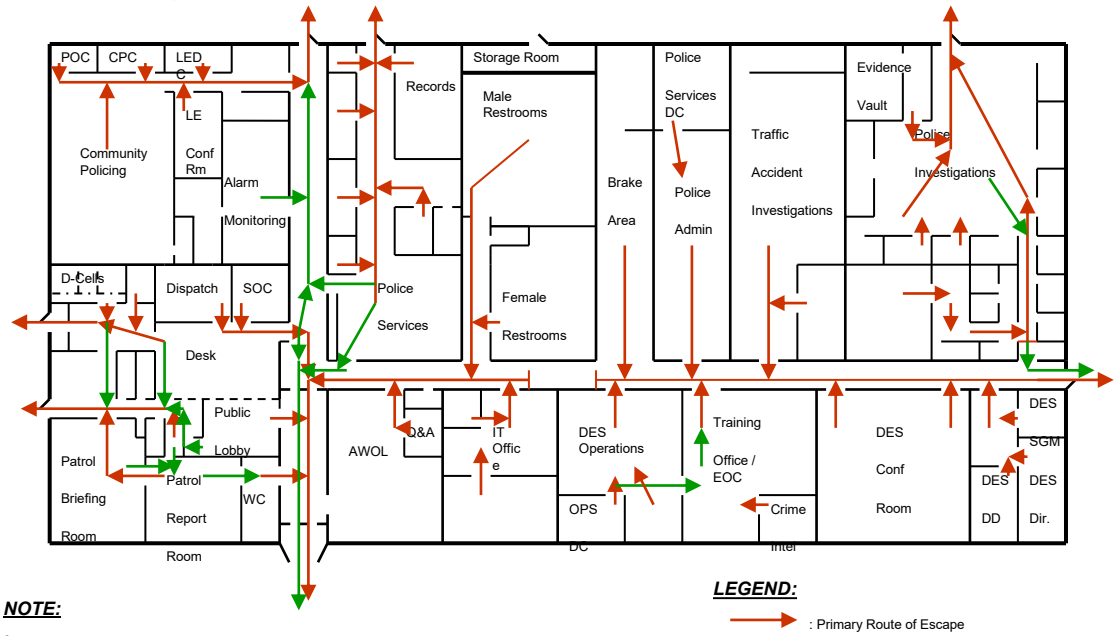
g. Once the AMS operator returns to the AMS area, make an assessment to the damage (if any) and notify the Contract Program Manager and the COR.

6. AMS operators will ensure that personal safety is the number one priority at all times.

Appendix E
Building 23020 Evacuation Map

BLDG 23020 Evacuation Plan

Directorate Of Emergency Services



NOTE:

- **All Prisoners will be evacuated under Armed Guard to the Employee Parking lot on the North Side of the Bldg.**

- **All Divisions / Branches will have an predetermined Accountability Location set up outside and at least 300 to 500 feet from the bldg. 1CD Museum Parking Lot is the Primary Site with the Health Clinic Parking Lot as the Secondary Site.**

LEGEND:

: Primary Route of Escape

: Alternate Route of Escape

Note: The above map will be used as a guide for any type of evacuation of building 23020.

Appendix F

Command Emergency Entrance Procedures

1. Command Emergency Entrance Procedures (CEEP) will be initiated by the unit commander or any officer or noncommissioned officer who is currently under "Assumption of Command Orders".

2. There is only one requirement for emergency entrance into an AA&E facility.

a. Personnel on the unaccompanied access roster are unavailable for whatever reason and the unit has a high priority mission requiring the use of AA&E that must be immediately accomplished.

b. Emergency entrance procedures WILL NOT be abused. Personnel returning or going to field or range operations, schools, etc. will not be considered an emergency. Failure to properly plan for events will also not be considered an emergency.

3. Commanders will use the following procedures for CEEP.

a. Commander will notify the AMS (287-7703) and inform the AMS operator that he/she is initiating Arms Room Command Emergency Entrance Procedures. The AMS operator will require a brief synopsis of the emergency. (Record in Shift Event Log)

b. The AMS operator will obtain the following information from the commander, Name, Unit, Building Number, Street Address, then notify the Police Desk to dispatch a Police Patrol to the Arms Room location. The Police patrol will meet with the commander there. This is not a priority call for the Police, ensure the Commander understands that they might have to wait until a Police Patrol is available.

c. The Police patrol will then verify the commander's identification, the patrol may ask to view the commander's assumption of command orders. Once the Police patrol is satisfied, same will contact the AMS monitor. The Police patrol may or may not stay at the scene. The AMS operator will then force the alarmed zone (arms room) to access. AMS operator will also force zone to secure, if requested by the Unit Commander.

d. The Commander will then take the sealed envelope, containing the alternate key to the primary arms room key box, open the envelope and retrieve the arms room entrance keys and arms room rack and container keys.

e. The Commander will then enter the arms room and conduct an immediate physical inventory of all AA&E (Weapons, Ammunition and Sensitive Items). This will be recorded on the armorer's opening inventory form (DA Form 2062). If this form is unavailable, the Commander will record it on a separate sheet of paper. Once the physical inventory is completed, the Commander, while remaining in the arms room, can direct only the necessary amount of personnel to issue AA&E. (The Commander can elect to conduct the issue him/herself) AA&E will be issued IAW AR 710-2, DA PAM 710-2-1, and AR 190-11.

f. Once the mission is either completed or one of the armorers that are on the unaccompanied access roster return, a Command Directed 100% by serial number inventory will be completed by a Staff Sergeant or above. The Commander will then author a memorandum stating the circumstances behind the CEEP and the actions taken, to include any discrepancies. This memorandum will be signed by the Commander, attached to the 100% serial number inventory and retained on file in the arms room for 2 years. A copy of the memorandum, 100% serial number inventory will be forwarded to the units S-2 and the DES Physical Security Branch Chief.

g. The primary armorer will also conduct a 100% inventory of all AA&E, to include sensitive items as soon as possible. This inventory will be attached with the command 100% serial number inventory and retained on file for 2 years.