Headquarters
1st Infantry Division and Fort Riley
Fort Riley, Kansas 66442

*FR Regulation 190-11

Date: 24 SEP 2010

Directorate of Emergency Services

THE INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEM

1. PURPOSE. This regulation outlines policy, prescribes procedures, and assigns responsibilities for the proper use of the Integrated Commercial Intrusion Detection System (ICIDS) and related physical security equipment installed on Fort Riley.

2. REFERENCES. Required and related publications and prescribed and referenced forms are listed in Appendix A.

3. SUGGESTED IMPROVEMENTS. The proponent agency of this regulation is the Directorate of Emergency Services, Physical Security Division. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Director, Directorate of Emergency Services, ATTN: IMWE-RLY-ES, 221 Custer Avenue, Fort Riley, Kansas 66442.

4. EXPLANATION OF ABBREVIATIONS AND TERMS. Abbreviations and special terms used in this regulation are explained in the glossary.

5. APPLICABILITY. This regulation applies to all units and activities assigned or attached to Fort Riley.

6. RESPONSIBILITIES.

a. The Directorate of Emergency Services (DES), Chief, Physical Security Division, ICIDS Program Manager for Fort Riley will:

(1) Coordinate IDS requirements with the Network Enterprise Center (NEC), the Directorate of Logistics (DOL), the Directorate of Public Works (DPW), and the U.S. Army Corps of Engineers, District Office of Fort Riley, as appropriate, for installations of ICIDS.

---

* This regulation supersedes FR Regulation 190-11, dated 1 December 2008.

(2) Prepare and submit to the Installation Management Command (IMCOM), ICIDS site survey requests for projects that exceed Fort Riley capabilities.

(3) Identify requirements for ICIDS to protect installation facilities ensuring the following guidance is followed:

(a) Review all ICIDS requests, ensuring all requests meet higher headquarters guidelines and requirements outlined in AR 190-11 (Physical Security of Arms, Ammunition, and Explosives), AR 190-13 (The Army Physical Security Program), and AR 190-51 (Security of Unclassified Army Property (Sensitive and Non-sensitive)).

(b) Identify ICIDS requirements and needs by conducting physical security surveys and inspections, reviewing military construction (MILCON) projects, and reviewing specific requests from installation activities and units.

(c) Conduct a risk analysis on existing facilities in accordance with DA Pam 190-51 (Risk Analysis for Army Property) and AR 190-51 to determine whether ICIDS requirements exist as part of the physical protective measures outlined in AR 190-51, para 3-3e.

(4) Conduct acceptance testing of all new ICIDS installations or modifications at all activities on Fort Riley.

(5) Initiate all ICIDS service requests and work orders to DOL.

(6) Input and create all new zones into the ICIDS database.

(7) Develop a training and certification program for all new military and civilian dispatchers.

(8) Review all ICIDS event logs to determine whether or not the dispatchers are performing their duties to standards. All discrepancies will be reported to the Dispatcher Supervisor and the ICIDS Program Administrator.

(9) Verify the unit or activity access rosters and background investigation (if required) prior to issuing a six digit Personal Identification Cipher (PIC) and a four digit Personal Identification Number (PIN) to the user.

(10) Conduct training for ICIDS users on how to properly enter their PIC/PIN numbers to access and secure their ICIDS zone.

b. The Directorate of Public Works (DPW) will identify facilities, plans, and projects to the DES, Physical Security Division for consideration of ICIDS requirements.

c. The Network Enterprise Command (NEC) will:

(1) Provide technical assistance concerning transmission lines and connections of ICIDS to transmission lines.

(2) Program transmission lines and equipment to support all current and future ICIDS requirements.

(3) Install and maintain transmission lines for ICIDS.

d. The Directorate of Logistics (DOL) will:

(1) Install, remove, repair and provide preventive maintenance for all government owned ICIDS. All requests for ICIDS maintenance and repair must be reviewed and submitted by DES, Physical Security Division or on duty dispatchers. Maintenance requests submitted directly by ICIDS users will not be processed.

(2) Program funds to support installation, maintenance and repair of ICIDS.

(3) Order and issue ICIDS and components for replacement and maintain records for equipment accountability, including an updated price list for ICIDS parts and components.

(4) Ensure that installation and maintenance personnel undergo required security checks in accordance with AR 190-11, para 3-6l (2-4).

(5) Ensure that installation, maintenance and repair personnel can be reached by pager or telephone during normal duty hours and non-duty hours and respond within two hours for emergencies.

(6) Maintain DD Form 314 (Preventive Maintenance Schedule and Record) for all systems. All maintenance and repair performed will be documented on a DA Form 2407 (Maintenance Request) initiated from the Maintenance Division, DOL, 8100 1st Division Rd. All ICIDS installations, moves or alterations will be documented on DA Form 4604 (Security Construction Statement) and provided to the ICIDS user verifying technical acceptance of the operations of ICIDS.

(7) Conduct semi-annual maintenance and testing of each ICIDS system per AR 190-11, para 3-6m (3-4). The results of the semi-annual maintenance conducted will be annotated on DD Form 314 (Preventive Maintenance Schedule and Record) maintained by the maintenance personnel.

e. Responsible Officers of IDS protected facilities (AA&E and Non-AA&E) will:

(1) Provide an access roster of all persons granted unaccompanied access to the Arms, Ammunition and Explosives (AA&E) or Non-AA&E facilities protected with

ICIDS. Access roster will be immediately updated whenever a change in personnel, information or Commander/manager occurs. At a minimum, the access roster will be updated semi-annually. The access roster will be posted on the interior wall of the protected zone, out of view of personnel not authorized in the protected area.

(2) Instruct all personnel listed on the unaccompanied access roster to report to DES, Physical Security Division, 221 Custer Avenue, to obtain their PIC/PIN number. The PIC/PIN numbers will be issued from 0900-1500 hrs Monday thru Friday. The system will assign a six digit Personnel Identification Cipher (PIC) and the individual will select their own private four digit Personal Identification Number (PIN). It is not acceptable to use the last four numbers of their Social Security Number, sequential numbers, for example, 1234 or identical numbers, such as 1111. The PIC/PIN numbers will not be issued or given out over the telephone or via e-mail.

(3) Ensure that procedures are addressed in the unit or organization Standard Operating Procedure (SOP) to protect an individual's PIC/PIN from being shared with other persons or otherwise compromised. Intentionally compromising PIC/PIN numbers is a violation of this regulation. Violations of the provisions of this regulation will be processed as follows:

(a) Military personnel who violate the provisions of this regulation will be subject to prosecution under Article 92 of the Uniform Code of Military Justice or appropriate administrative action.

(b) Civilians who violate the provisions of this regulation are subject to appropriate administrative action.

(4) In the event a PIC/PIN number is compromised by sharing it with another person or otherwise intentionally compromising it, all PIC/PIN numbers assigned to the protected zone will be removed from the zone pending the receipt of an updated access roster and a memorandum signed by the first Battalion Commander or Director in the chain of command stating the steps the unit has taken to prevent the violation from reoccurring. New PIC/PIN numbers will then be issued to all zone users.

(5) If a PIC/PIN is inadvertently lost and it is suspected that it might be compromised, the person assigned the PIC/PIN should immediately report the compromise to the ICIDS Administrator and request the old PIC/PIN be withdrawn and a new PIC/PIN issued.

(6) Ensure that unit or activity personnel do not attempt to service or tamper with any ICIDS components. When remodeling, repairing, or painting requires removal or relocation of ICIDS, notify the Physical Security Division at 239-6342 or 239-3528 and request assistance. **DO NOT ATTEMPT TO MOVE THE SENSORS ON YOUR OWN.** When painting is required, **DO NOT PAINT** over any ICIDS sensors, components, key pads, control panels, conduit, or cables.

(7) Ensure the ICIDS is tested at least once every 30 days and the results of the test are recorded on the unit's or activity's DA Form 4930. Completed forms must be retained on file for one year. This monthly testing requirement is for all ICIDS zones.

f. Responsible Officers of AA&E facilities will:

(1) Ensure that personnel (enlisted, civilian and contractors) requiring unaccompanied access to AA&E storage facilities have been properly screened using a DA Form 7281, Command Oriented Arms, Ammunition, and Explosives (AA&E) Security Screening and Evaluation Record as required by AR 190-11, para 2-11, prior to being granted unaccompanied access. Directors may delegate this responsibility to managers or the contract officer's representatives who are directly responsible for the supervision of personnel and AA&E. The following guidance is provided for clarification:

(a) Commissioned officers are not required to be screened and may be granted unaccompanied access to the AA&E storage facility provided they are listed on the unaccompanied access roster signed by the unit Commander.

(b) Complete a DA Form 7281 on personnel previously screened and granted unaccompanied access while assigned to a different unit prior to being granted unaccompanied access in their current unit of assignment. The use of screening records completed by a Commander of a different unit is not authorized for granting unaccompanied access to AA&E.

(c) Review and update unaccompanied access roster upon assumption of command.

(d) Attach a memorandum to the DA Form 7281(s) identifying the Soldier(s) and/or civilian(s) by the name of the individual and the last five numbers of their social security number. The memorandum will ensure the correct records are checked. The sample memorandum provided at figure 4 will be used for preparing the memorandum.

(2) Provide the DES, ICIDS System Administrator with an unaccompanied access roster (original signature) for each AA&E storage facility. An example of an unaccompanied access roster for AA&E facilities may be found at figure 1. Ensure:

(a) As a minimum all unaccompanied access rosters are updated anytime there is a change in personnel granted unaccompanied access or semi-annually whichever time is shorter.

(b) Copies of the completed DA Forms 7281 for persons on the unaccompanied access roster are provided to the ICIDS System Administrator.

(3) Ensure that personnel secure (activate the ICIDS) their arms room during any period the arms room is not physically manned by someone listed on the unaccompanied access roster; this includes latrine breaks, and lunch break. Use of a

locked day gate or vault door without activating the ICIDS does not constitute a secured arms room.

(4) Ensure a 100% physical count inventory is conducted anytime the arms room keys change possession. For the purposes of this regulation, keys change possession whenever they are transferred between individuals on the unaccompanied access roster or they are locked in or retrieved from a container used for overnight storage. The results of the inventory will be recorded on a DA Form 2062 by NSN and maintained until the next serial number inventory has been completed without discrepancies.

(5) When ICIDS is no longer required and all weapons and sensitive items have been removed by the existing unit, a closeout memorandum signed by the Commander will be turned into the Physical Security Division. The sample memorandum provided at figure 3 will be used for preparing the closeout memorandum.

g. Responsible Officers of Non-AA&E facilities will provide the ICIDS System Administrator with the unaccompanied access roster (original signature required) for each facility protected by ICIDS. All access rosters for non-AA&E facilities will be updated when there is a change to the roster, when there is a change in facility manager or semi-annually whichever time is shorter. Access rosters that do not follow the example provided in figure 2 will not be accepted. Personnel requiring access to pharmacy facilities must provide written documentation showing they have been interviewed by the lowest level Commander responsible for the security of the pharmacy. The PIC/PIN numbers will not be issued without this documentation.

h. Special Security Office (SSO) will appoint an individual to serve as the Super Sensitive Compartmented Information Facility (SCIF) ICIDS Administrator. The Super SCIF ICIDS Administrator will be responsible for issuing PIC/PIN numbers to all SCIF users, submitting maintenance requests through the Fort Riley ICIDS Administrator, and maintaining the ICIDS database for all SCIF nodes. A copy of the appointment orders will be provided to the Fort Riley ICIDS Administrator.

7. INSTALLATION AND MAINTENANCE OF INTEGRATED COMMERCIAL INTRUSION DETECTION SYSTEMS (ICIDS).

a. The installation and maintenance of ICIDS will be based on priority established in Army regulation, IMCOM operation order and this regulation. The Installation ICIDS is a security resource with limits based on initial cost, current system capacity, monitoring capability, annual maintenance costs and available response assets. The requirement for ICIDS must be documented. Priority for ICIDS installation is based on Table 4-1 and 4-2, AR 190-13:

(1) Special Compartmented Information Facilities.

(2) Arms, Ammunition and Explosives (Category I through IV).

(3) Radiation Storage.

(4) Critical communication network hubs.

(5) Pharmacies.

(6) Physical protective measure required after conducting a risk analysis resulting in a Risk Level III.

(7) ICIDS support provided to partner organizations, i.e. National Guard, ASOS, AAFES, MEDDAC and DECA and supported by an inter-service support agreement.

(8) Other areas recommended by regulation when other protective measures are not practical.

b. Work Orders/Service Orders.

(1) Telephone work order request will be submitted by the Physical Security Division via Remedy to NEC no more than 21 days in advance of the expected project start date. Work order priority will be established by the Physical Security Division with NEC concurrence.

(2) The Physical Security Division will submit work/service orders to DOL via the DOL work order line for ICIDS installation and maintenance.

c. Operational Testing. Initially, each sensor and duress switch shall be individually tested by ICIDS installers. Each sensor shall be tested until all detection zones can be certified as operating properly. After system certification, the entire integrated system will be tested to assure that all sub-elements are compatible and function as a complete system.

8. STANDARDS FOR ICIDS OPERATIONS.

a. All facilities protected with ICIDS will be set to require entry of a PIC and PIN. The use of both the PIC and PIN allows for the added benefit of a built in duress feature of the ICIDS system. The duress feature can be activated by entering the last number of a PIN off by one number. (**Example**: PIN of 1235 entered as 1234 or 1236 will activate duress.)

b. The default time period for ROUTINE ACCESS to areas protected with ICIDS is 0600 hours to 1800 hours. During the routine access period, personnel are required to deactivate the ICIDS system on entry into the protected area and to alarm the system when exiting. No additional measures are required to remain in the protected area within the routine access period. Anytime access is necessary outside the routine access period, the user must request EXTENDED ACCESS by entering or re-entering his/her PIC and PIN for each additional hour of access.

c. A Commander or Director may request the ROUTINE ACCESS period be adjusted if a unit or activity's normal hours of operation differ from the default hours. This may be accomplished by annotating the unit or activity's normal hours of operation on their unaccompanied access roster. At no time will the period for routine access be granted for 24 hour operations except when the ICIDS is for duress purposes only.

d. Monthly ICIDS Tests. Units, directorates and activities will conduct operational testing of ICIDS monthly. The test will be initiated by calling the Alarms Monitoring Station at 239-3059. The dispatcher will then issue the user verbal instructions over the phone on how to test each sensor. All facilities equipped with the foot pedal duress will only be tested during a physical security inspection by the Physical Security Inspector. The monthly ICIDS test will be annotated on the DA Form 4930 and the log retained in the unit or activity files for one year.

e. Alarm Activations.

(1) Upon receipt of an alarm, the dispatcher will evaluate the information displayed and dispatch a patrol for further investigation if necessary or, if appropriate, attempt a remote reset.

(2) The dispatcher will request unit/activity personnel to respond to the protected area for the following reasons:

(a) when directed by the responding patrol,

(b) when the system cannot be remotely reset,

(c) when on battery back-up as a warning order of possible system failure (to be prepared to post armed guards for AA&E), or

(d) when the system has failed. (Post an armed guard for AA&E.)

(3) The dispatcher will contact unit/activity personnel based on information provided on the most current access roster.

(4) Failure to comply with the dispatcher's request to respond will result in the following actions.

(a) Immediate notification of the next higher headquarters for ICIDS protecting AA&E. For ICIDS protecting non-AA&E, monitoring will be suspended and a follow-up memorandum for record will be sent to the Battalion Commander or activity Director detailing the fact the user failed to comply with the request.

(b) The second incident of unit/activity personnel refusing to comply with the dispatcher's request to respond will follow the previous paragraph and will require a reply by endorsement from the Commander/activity chief/Director explaining corrective actions taken to ensure proper response in the future.

(c) The third incident for non-AA&E facilities protected with ICIDS may result in the termination of services and removal of the ICIDS from the facility.

9. INSPECTION OF ICIDS DURING PHYSICAL SECURITY INSPECTIONS. Physical security inspectors will:

a. Check unit or activity ICIDS by observing the user conduct both a test of the system and a test of the duress switch. Duress switches will only be tested by Physical Security Inspectors or at the direction of the dispatcher.

b. Inspect ICIDS components, visible transmission lines, cables and conduit for evidence of tampering.

c. Inform the ICIDS System Administrator of all sensors or switches that do not operate properly who will in-turn contact the ICIDS maintenance personnel to schedule repairs or adjustments.

d. Inspect the unit or activity's log entries and records regarding operation and inspection of ICIDS over the past year to include inspection records of higher headquarters.

10. AFTER HOUR SECURITY CHECKS.

a. After hour security checks are required on all AA&E storage facilities and will be conducted by unit personnel (CQ or Staff Duty) at least once every 8 hours. Activities without CQs or Staff Duty personnel must make arrangements to ensure their facilities are checked at the required frequency. All security checks will be annotated on Standard Form 702 (Security Container Checklist) and maintained on file for 90 days.

b. After hour security checks are required on all pharmacies. Security checks will be conducted every four hours during non-duty hours and documented on a Standard Form 702 (Security Container Checklist) and maintained for 90 days. Checks will be conducted by unit personnel (CQ, or Staff Duty).

11. ICIDS FAILURE.

a. Units and activities storing AA&E are required to post armed guards in clear view of the entrance to the protected area in the event of ICIDS failure.

(1) A guard is considered armed when in possession of the guard's assigned weapon and ammunition for that weapon.

(2) Commanders will ensure an operational load of ammunition is on hand and stored in the arms room. This will be accomplished by completing an ammunition site license packet, drawing the ammunition and properly accounting for it and storing it in

the arms room. Further information on ammunition site licenses can be obtained from the Garrison Safety Office or by calling 239-2245. It is recommended that units maintain a minimum of 450 rounds for their operational load to cover all possible requirements, armed guards for arms rooms without operational ICIDS, on and off post weapon and ammo escort requirements and ammo security detail at the AHA.

(3) Activities storing AA&E without the organic assets to post armed guards (ASP, bulk weapon storage facilities, museum, etc.) will coordinate armed guard support with the Division/MSE.

(4) Activities storing only category IV arms in a certified arms vault or a GSA-approve Class V storage container (AAFES and DFMWR) are not required to post armed guards but must check the facility at least once every 24 hours at irregular intervals.

(5) Commanders of units providing armed guards will follow procedures outlined in AR 190-14, Chapter 2. This includes and is not limited to:

(a) Written authorization by a field grade officer or higher or civilian equivalent GS-12 or above to carry the firearm.

(b) Mandatory training and proficiency testing within the preceding 12 months including use of force training.

b. Other facilities (non AA&E) normally protected with ICIDS will follow procedures outlined in their governing regulations.

(1) Pharmacies are required to have unarmed guard surveillance with the ability to contact the police dispatch center.

(2) Open storage facilities are required to have cleared guards or duty personnel check the protected area once every four hours.

(3) Other facilities may only require notification of ICIDS failure or may need to increase after hour security checks.

REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT AGENCY
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT RILEY
500 HUEBNER ROAD
FORT RILEY, KANSAS 66442-5000

OFFICE SYMBOL (Date)

MEMORANDUM FOR Director of Emergency Services, ATTN: ICIDS Administrator, Fort Riley, Kansas 66442

SUBJECT: Unaccompanied Access Roster

1. The following personnel are authorized unaccompanied access to, **(Building 0000, Zone 000)**, and to operate and test the ICIDS, and sign for the arms room keys of (name of unit)

NAME (**Alphabetical Order**)		RANK	ID NUMBER	POSITION
DO, Jane F.	SPC	(**Last 5 SSN**)		Armorer
HALE, Nathan	PFC	1-2345		Ast Armorer
PETERSON, Willie R	2LT	5-6789		AA&E Officer

2. Above named personnel have undergone a command developed security screening DA Form 7281-R (Command Oriented Arms, Ammunition, and Explosive {AA&E} Security Screening and Evaluation Record).

3. Unit Identification Code (UIC): _____

4. In the case of alarm activation call the following numbers:
Duty hours: 239-XXXX/XXXX, building #_____
After duty hours: SDO/SDNCO 239-XXXX/XXXX, building #_____

5. Alternate Contact Information:
Commander's Email Address: james.t.kirk@conus.army.mil Phone: 239-XXXX
First Sergeant's Email Address: michael.jones@conus.army.mil Phone: 240-XXXX

6. In the event that the armorer is unavailable, I authorize the DES to direct the SDO/SDNCO to contact company personnel by use of the unit alert roster.

SIGNATURE BLOCK

Figure 1. Sample Unaccompanied Access Roster for AA&E Facilities

REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT AGENCY
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT RILEY
500 HUEBNER ROAD
FORT RILEY, KANSAS 66442-5000

OFFICE SYMBOL (Date)

MEMORANDUM FOR Director of Emergency Services, ATTN: ICIDS Administrator, Fort Riley, Kansas 66442

SUBJECT: Unaccompanied Access Roster

1. The following personnel are authorized unaccompanied access to **Building 0000, Zone 000**, and to operate and test the Integrated Commercial Intrusion Detection System (ICIDS).

NAME **(Alphabetical Order)**	ID NUMBER **(Last 5 SSN)**	POSITION
DO, Jane F.		Manager
HALE, Nathan	1-2345	Asst. Manager

2. Above name personnel have been trained and know how to properly operate and test the ICIDS and control all facility keys.

3. Alternate Contact Information:
Managers' Email Address: Jane.Do@us.army.mil Phone: 239-XXXX
Asst Manager's Email Address: Nathan.Hale@conus.army.mil Phone: 240-XXXX

4. Unit Identification Code (UIC):

5. Hours of Operation are: 0600-2100 hrs

6. In the event of an alarm activation, I authorize the Directorate of Emergency Services (DES) to call the following personnel in order of listing:

Name	**Duty Phone Number**	**Home Phone Number**
Jane Do	239-1111	(785) 555-5555

SIGNATURE BLOCK

Figure 2. Sample Unaccompanied Access Roster for non-AA&E Facilities

REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT AGENCY
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT RILEY
500 HUEBNER ROAD
FORT RILEY, KANSAS 66442-5000

OFFICE SYMBOL (Date)

MEMORANDUM FOR Director of Emergency Services, ATTN: IMWE-RLY-ESS (ICIDS System Administrator), 221 Custer Ave., Fort Riley, Kansas 66442

SUBJECT: Deactivation of Installation Commercial Intrusion Detection System (ICIDS) for (Unit Name), (Building 0000, Zone 000)

1. The following memorandum is for deactivation of the ICIDS in Bldg 0000, Zone 000. It has been cleared of all Arms, Ammunition, and Explosives (AA&E) and sensitive items and is no longer in use.

2. The combination on the vault door has been reset to the factory default setting of 50-25-50. ***(NOTE: This line can be omitted if the facility utilizes a high security padlock).***

3. POC for this memorandum is the undersigned at 239-XXXX.

Signature block

Figure 3. Sample Closeout Memorandum for AA&E Facilities

REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT AGENCY
HEADQUARTERS, UNITED STATES ARMY GARRISON, FORT RILEY
500 HUEBNER ROAD
FORT RILEY, KANSAS 66442-5000

OFFICE SYMBOL (Date)

MEMORANDUM FOR RECORD

SUBJECT: Local Records Check

1. The following personnel are being considered for duties involving arms, ammunition, and explosives (AA&E). Request that local records checks be conducted on these individuals and the results be recorded on the enclosed DA Form 7281-R (Command Oriented Arms, Ammunition, and Explosives (AA&E) Security Screening and Evaluation Record).

NAME	ID NUMBER
DO, Jane F.	(**Last 5 SSN**)
HALE, Nathan	1-2345

2. Point of contact for this memorandum is the undersigned at 239-XXXX.

Encl
as

SIGNATURE BLOCK

Figure 4. Sample Memorandum for Local Records Check

APPENDIX A
References

Section I
Required Publications

AR 190-11
Physical Security of Arms, Ammunition and Explosives

AR 190-13
The Army Physical Security Program

AR 190-14
Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 190-51
Security of Unclassified Army Property (Sensitive and Nonsensitive)

UCMJ Article 92
Failure to Obey Order or Regulation

UFC 4-020-04 (TM 5-853-4)
Security Engineering, Electronic Security Systems

TM 5-6350-275-24&P
Unit, Direct Support and General Support Maintenance Manual Including Repair Parts and Special Tools List for the Integrated Commercial Intrusion Detection System (ICIDS)

Section II
Related Publications

No entries

Section III
Prescribed Forms

DA Form 2407
Maintenance Requests

DA Form 2806-1-R
Physical Security Inspection Report

DA Form 4604
Security Construction Statement

DA Form 4930
Alarm Intrusion Detection Record

DA Form 7281
Command Oriented Arms, Ammunition, and Explosives (AA&E) Security Screening and Evaluation Record

DD Form 314
Preventive Maintenance Schedule and Record

Standard Form 702
Security Container Checklist

Section IV
Referenced Forms

DA Form 2028
Recommended Changes to Publications and Blank Forms

GLOSSARY

AA&E
Arms, Ammunition and Explosives

DES
Directorate of Emergency Services

DOL
Directorate of Logistics

DPW
Directorate of Public Works

ICIDS
Integrated Commercial Intrusion Detection System

IMCOM
Installation Management Command

MILCON
Military Construction

MSC
Major Subordinate Command

NEC
Network Enterprise Command

PIC
Personal Identification Cipher

PIN
Personal Identification Number

SCIF
Sensitive Compartmented Information Facility

SOP
Standard Operating Procedure

UCMJ
Uniform Code of Military Justice

DAVID C. PETERSEN
Brigadier General, USA
Deputy Commanding General - Rear

OFFICIAL:

KENNETH F. STEGGEMAN
Director, Directorate of Human Resources

APPENDIX A – References
Glossary

DISTRIBUTION:

Fort Riley SharePoint