

Fort Knox Regulation 190-45

Military Police

**Fort Knox
Incident
Reporting**

Headquarters
US Army Garrison
Fort Knox, Kentucky 40121-5719
8 December 2015

UNCLASSIFIED

SUMMARY of CHANGE

Fort Knox Regulation 190-45
Incident Reporting

This major revision dated, 8 December 2015—

- o Renumbers Fort Knox Regulation 190-40, Incident Reporting, 15 April 2008, to Fort Knox Regulation 190-45 to parallel Army Regulation (AR) 190-45 (Law Enforcement Reporting).
- o Deletes all references to U.S. Army Armor Center and School (USAARMC) and replaces it with U.S. Army Cadet Command (USACC) to comply with the reorganization of the installation.
- o Reformats the regulation to comply with DA Pam 25-40, Army Publishing: Action Officers Guide including basic structure, appendices, tables, and charts.
- o Updates reporting responsibilities throughout the regulation to Commanding General, U.S. Army Cadet Command as the Senior Commander, to comply with the reorganization of the installation.
- o Updates Fort Knox reporting procedures to comply with updates to Army Regulation 190-45 (Law Enforcement Reporting), TRADOC Regulation 1-8 (U.S. Army Training and Doctrine Command Operations Reporting), and IMCOM Regulation 190-45-1 (United States Army Installation Management Command (IMCOM) Serious Incident Reports (SIRs) Commanders Critical Information Reports (CCIR)).
- o Updates reportable incidents to comply with updated guidance.
- o Updates serious incident report formats (chapter 3).
- o Updates and complies all references (appendix A).
- o Adds Management Control Checklist, (appendix B).
- o Updates reporting processes for personally identifiable information (PII) breaches, (appendix C).
- o Adds Suspicious Activity Reporting (SAR) requirements, (appendix D).
- o Adds Reporting Defense Support of Civil Authorities (DSCA), (appendix E)

Headquarters
US Army Garrison
Installation Management Command
Fort Knox, Kentucky 40121-5719

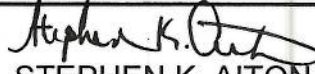
Fort Knox Regulation 190-45

8 December 2015

Military Police

Incident Reporting

OFFICIAL:


STEPHEN K. AITON
COL, AG
Commanding

History. This is a major revision of Fort Knox (FK) Regulation 190-40.

Summary. This regulation provides guidance on the notification and written reporting requirements for serious incident reports.

Applicability. All units, directorates, Partners in Excellence (Fort Knox tenant organizations), external units training on Fort Knox and Fort Knox Directorates are required to report incidents as outlined in this regulation. For the purpose of this regulation, the senior leader/supervisor for each organization will be addressed as commander.

Proponent and exceptions. The proponent and exception/waiver authority of this regulation is the Director, Directorate of Plans, Training, Mobilization and Security (DPTMS). The primary point of contact for questions is the on-duty watch officer at the Installation Operations Center (IOC), 502-624-2707/5151, usarmy.knox.imcom-atlantic.mbx.ioc-watch-ofcr@mail.mil

Army Management Control Process. This regulation contains management control provisions and identifies key management controls that must be evaluated in accordance with AR 11-2.

Supplementation. Supplementation of this regulation is prohibited without prior approval from the Directorate of Plans, Training, Mobilization, and Security (DPTMS) (IMKN-PLI-OC), Fort Knox, KY 40121-5717.

Suggested Improvements or Clarification. Users are invited to send comments and suggested improvements through their chain of command to the Installation Operations Center, DPTMS (IMKN-PLI-OC), Fort Knox, KY 40121-5717.

Distribution. Distribution of this regulation is intended for all organizations stationed at Fort Knox. Distribution is in electronic media only.

*This regulation supersedes FK Regulation 190-40, Incident Reporting, 15 April 2008.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction

Purpose • 1-1, *page 1*

References • 1-2, *page 1*

Explanation of abbreviations and terms • 1-3, *page 1*

Responsibilities • 1-4, *page 1*

Policy • 1-5, *page 4*

Chapter 2

Reporting Policy

General • 2-1, *page 4*

Reportable Incidents • 2-2, *page 4*

Chapter 3

Reporting Procedures

General • 3-1, *page 7*

Time and Reporting Requirements • 3-2, *page 8*

Commanding General's Update Requirements • 3-3, *page 11*

Appendixes

A. References, *page 14*

B. Management Control Checklist, *page 17*

C. PII Reporting, *page 18*

D. SAR Reporting, *page 19*

E. DSCA Reporting, *page 22*

F. AR 190-45 and AR 600-8-1, Reporting Areas of Responsibility, *page 24*

G. DPTMS IOC-Watch Officer Procedures for Reporting, *page 27*

Figure List

Figure 3-1: Incident Notification Flow Chart, *page 8*

Figure 3-2: Email EXSUM Format, *page 9*

Figure 3-3: Detailed SIR Report Format, *page 10*

Figure 3-4: CGs Update email EXSUM, *page 12*

Figure 3-5: CGs Update Report, *page 12*

Figure D-1: SAR Email EXSUM Format, *page 20*

Figure D-2: Detailed Report Format, *page 21*

Contents (continued)

Figure E-1: DSCA Support EXSUM Format, *page 23*

Figure F-1: AR 190-40 Fort Knox Area of Responsibility, *page 24*

Figure F-2: AR 600-8-1 Fort Knox Casualty Area of Responsibility, *page 25*

Glossary

Chapter 1

Introduction

1-1. Purpose

To establish policy and procedures for the reporting of significant incidents involving units, directorates, Partners in Excellence (Fort Knox tenant organizations), and external units training on Fort Knox and incidents within the Fort Knox area of responsibility (AOR) in appendix E. The primary purpose of this process is to provide a means to inform the Fort Knox senior leadership, Training and Doctrine Command (TRADOC), Installation Management Command (IMCOM), Installation Management Command – Atlantic Region (IMCOM-AT) and Headquarters, Department of the Army (HQDA) (and other headquarters as required) of incidents which impact Fort Knox elements and personnel.

1-2. References

The primary sources for reporting requirements are the required and related publications, as well as prescribed and referenced forms listed in appendix A. In addition, reporting requirements are found in the published Commander's Critical Information Requirements (CCIRs) from TRADOC, IMCOM, First U.S. Army, U.S. Army Forces Command (FORSCOM), U.S. Army Northern Command (ARNORTH); the Commanding General, U.S. Army Cadet Command (USACC) and Fort Knox, and other commanders. These CCIRs, updated frequently by the respective commanders, are sensitive and therefore not listed in this document. A detailed list of references is in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and terms used in this regulation are explained in the glossary.

1-4. Responsibilities

- a. Commanding General (CG), U.S. Army Cadet Command.
 - (1) Serve as Senior Commander (SC) Fort Knox for all reporting in accordance with (IAW) AR 190-45 and TRADOC Regulation 1-8.
 - (2) Designate Fort Knox Installation Operations Center (IOC) as executive agent for reporting to higher headquarters.
- b. Commanders, Units, and Directorates Reporting Directly to Headquarters, U.S. Army Cadet Command.
 - (1) Immediately, upon determination/discovery of a reportable incident, follow the procedures established by CG, USACC for reporting.
 - (2) Ensure the USACC staff notifies the IOC of all category (CAT) 1, 2 and 3 reportable incidents including those from Cadet Summer Training (CST) and Cultural Understanding & Language Proficiency (CULP).
 - (3) Respond to requests for information (RFI) from the IOC and support staff.
- c. Commanders, Partners in Excellence (Fort Knox Tenant Organizations). (For additional/specific requirements, see para 1-4, d-f.)
 - (1) Ensure that the policies and procedures of this regulation are implemented.
 - (2) Immediately, upon determination/discovery of a reportable incident, follow the

procedures dictated by your next higher headquarters.

(3) Provide the IOC a courtesy copy of all associated reports sent to higher headquarters for all personnel living and/or working on Fort Knox and those incidents occurring within the Fort Knox AR 190-45 reporting AOR (appendix F) in order to keep the USACC command group and the Garrison Commander (GC) informed. Use email executive summary (EXSUM) (figure 3-2 with report attached).

(4) Report incidents to the SC in a timely manner. Telephonic notification to the IOC must be made immediately or within 1 hour of the incident if there is a loss of weapon, life, limb, or eyesight; report within 2 hours for all other incidents.

(5) Respond to RFI from the IOC and support staff.

(6) Notify the Fort Knox Casualty Section directly for all incidents involving loss of life, limb, eyesight, or hospitalization for additional assistance.

(7) Submit requests for additional support (including chaplain, Public Affairs Office (PAO), law enforcement liaison, etc.) to the IOC.

(8) For incidents involving Soldiers, Civilians, and Family Members assigned and/or working/residing on Fort Knox that concern the loss of life, limb or eyesight and any other incident the commander deems necessary, submit a CG's Update (para 3-3).

d. External Units Training on Fort Knox (Regardless of Unit Size):

(1) Immediately upon determination/discovery of a reportable incident notify Range Control. Radio and/or telephonic notification to range control must be made immediately.

(2) Immediately, upon determination/discovery of a reportable incident, follow the procedures dictated by your higher headquarters.

(3) In order to keep the USACC command group and GC informed, provide a courtesy copy of all incident reports and associated reports to the IOC through range control. The IOC and range control will assist with any administrative resources necessary to produce the report and notify appropriate personnel/headquarters.

(4) Submit requests for needed support (chaplain, casualty assistance, public affairs, law enforcement liaison, etcetera) to the IOC.

(5) Respond to requests for information (RFI) from Range Control or the IOC.

e. Commander, U.S. Army Medical Department Activity (MEDDAC) and Ireland Army Community Hospital (IACH), Fort Knox.

(1) Ensure that the policies and procedures of this regulation are implemented.

(2) Provide information to the IOC (the SC's executive agent for reporting) on the patients involved in a reportable incident as allowed.

(3) Provide courtesy copies of all reports sent through MEDDAC channels to higher headquarters that are associated with an ongoing or reportable incident to the IOC.

(4) Report any reportable incident concerning Warrior Transition Unit (WTU) Soldiers or cadre to the IOC and Fort Knox leadership.

(5) Report anytime a military or garrison support entity is dispatched off post to assist civilian authorities under any agreement or regulatory requirement (appendix E).

(6) Provide information to the unit commander for the CG's Update.

(7) Respond to RFI from the IOC.

f. Commander, 703rd Explosive Ordnance Disposal (EOD) Detachment, Fort Knox.

(1) Ensure that the policies and procedures of this regulation are implemented.

(2) Report to the IOC anytime an EOD entity is dispatched off post to assist civilian

authorities under any agreement or regulatory requirement (appendix E).

(3) Respond to RFI from the IOC.

g. Commanders, Units, and Directorates Reporting Directly to Headquarters, U.S. Army Garrison (IMCOM) Fort Knox. (Additional/specific directorate requirements can be found in para 1-4(h-k.)

(1) Ensure that the policies and procedures of this regulation are implemented.

(2) Report incidents in a timely manner.

(3) Respond to RFI from the IOC and support staff.

(4) Directors and staff must ensure the appropriate Headquarters and Headquarters Company (HHC) or equivalent level commander and/or first sergeant is informed if a Soldier is involved.

(5) Directors/Staff are not authorized to report SIR incidents to higher headquarters staffs until approved by the GC.

(6) Conduct trend analysis and provide feedback on identified trends to the leadership and SC.

h. Directorate of Plans, Training, Mobilization, and Security – IOC.

(1) Act as executive agent for reporting on behalf of the SC, CG, USACC.

(2) Comply with the procedures outlined in this regulation and the “Watch Officer Incident Reporting Procedures” standing operating procedures (SOP) upon notification of a reportable incident. (The SOP may be more up-to-date with changing guidance; this regulation may be in revision.)

i. Directorate of Human Resources (Casualty Assistance Center (CAC)).

(1) Follow appropriate regulatory guidance and SOPs.

(2) Provide a courtesy copy of casualty reports to the IOC.

(3) Provide information to the unit commander for the CG’s Update.

(4) Respond to RFI from the IOC.

j. Directorate of Emergency Services (DES).

(1) Submit any acknowledgement of current or planned investigations associated with a reportable incident to the IOC.

(2) Report anytime a military or garrison support entity is dispatched off post to assist civilian authorities under any agreement or regulatory requirement (appendix E).

(3) Provide information to the unit commander for the CG’s Update.

(4) Respond to RFI from the IOC.

k. Public Affairs Office (PAO).

(1) Provide information and advice pertaining to the release of information to the IOC and command group concerning incidents.

(2) Provide a courtesy copy of all press releases associated with reportable incidents to the IOC.

(3) Provide information to the unit commander for the CG’s Update.

(4) Respond to RFI from the IOC.

l. Safety Officer.

(1) Provide information on any safety concerns associated with a reportable incident to the IOC.

(2) Provide courtesy copies of all reports sent through safety channels to a higher headquarters that are associated with an ongoing reportable incident to the IOC.

(3) Provide information to the unit commander for the Commanding General's Update.

(4) Respond to RFI from the IOC.

1-5. Policy

a. The commander/director of the person related to the report (whether victim, subject, Soldier, civilian, Family member or contractor) is responsible for the reporting process. Information on the incident may come from a variety of sources: the hospital, DES, Range Division, Criminal Investigation Division (CID), local law enforcement, etcetera.

b. Report incidents concerning personnel assigned to or residing on Fort Knox and those within the Fort Knox reporting AOR (appendix F). In addition, report incidents for personnel with temporary duty to Fort Knox including personnel training on Fort Knox. This includes cadets on Fort Knox for training or school. When considering if the incident is reportable, commanders should use the thought process "who else needs to know?"

c. Incident reporting correspondence is considered for official use only (FOUO) and the appropriate safeguards/ precautions for dissemination and distribution must be made IAW Army guidelines.

Chapter 2 Reporting Policy

2-1. General

a. Report incidents to the Fort Knox IOC, as defined in paragraph 2-2 and Appendix D. The lists are not inclusive. Commanders should report any incident that might concern the Fort Knox SC as a serious incident, regardless if specifically listed ("who else needs to know"). In determining whether an event/incident is of concern to the SC, the following factors should be considered: severity of the incident, potential for adverse publicity, potential consequences of the incident, whether or not the incident is reportable under other reporting systems, and/or effect of the incident on readiness or the perception of readiness. If in doubt, submit an incident report.

b. Reporting procedures outlined in this regulation do not replace the reporting procedures outlined in AR 190-45 (Law Enforcement Reporting), Army Command (ACOM) reporting requirements, or the submission of other reports (for example, aviation or ground accident reports submitted through separate reporting channels). Parallel reports are often required due to separate reporting channels. Commanders at all levels will report alleged criminal incidents to the DES and/or CID for appropriate inquiry and investigation.

2.2. Reportable Incidents

Fort Knox SIRs are derived from multiple sources; however, primary sources are SIRs per AR 190-45, TRADOC 1-8, IMCOM 190-45-1, and CCIRs from TRADOC, IMCOM, FORSCOM, ARNORTH, and CG Fort Knox.

- a. Report all SIR CAT 1 & 2 reportable incidents listed in AR 190-45.
- b. Report the incidents below as CAT 3.
 - (1) SC Fort Knox CCIR as updated and provided by the IOC.
 - (2) Training use of riot control agent or chemical/biological stimulants outside of established parameters.
 - (3) Death or serious injury to a Fort Knox Soldier or Department of the Army Civilian (DAC) (on or off post), as well as Fort Knox Soldier, immediate Family member, DAC contractor or other civilian on post.
 - (4) Serious crime (that is, aggravated assault, sexual assault, rape, larceny exceeding \$50,000, and murder or attempted murder) on or off the installation committed by or against a Fort Knox Soldier, Family member, DA Civilian, contractor, Future Soldier, or contracted Senior Reserve Officers' Training Corps (ROTC) Cadet. This also applies to any Senior ROTC cadet while in training status. Additionally, all sexual assault cases are required to be entered into Defense Sexual Assault Incident Database (DSAID) upon notification and the DSAID number entered in the SIR line 13, or "Unknown" for each case entered. Only unrestricted reports of sexual assault or rape will be reported through these channels, see special instructions in paragraph 3-2a(2).
 - (5) Significant environmental injury to Fort Knox Soldiers, dependents, or DA Civilians (such as, heat stroke, rhabdomyolysis, heat exhaustion, carbon monoxide poisoning, hypothermia, frostbite, and communicable illnesses, such as, influenza, hepatitis, and West Nile virus). Consult with medical personnel may be required for proper diagnosis of the injury. Report possible cases and provide follow up report with appropriate diagnosis.
 - (6) Communicable illnesses that exceed the expected baseline for those illnesses and unusual illnesses. Consult with the local medical treatment facility.
 - (7) Suicide attempts (all overt acts of self-destructive behavior that do not result in death) occurring on the installation and suicide attempts by a Soldier, dependent, or DA Civilian occurring off the installation. (See DA Pam 600-24 for suicide prevention information).
 - (8) Any reportable incident or event involving Soldiers assigned or attached to the Warrior Transition Unit (WTU) on Fort Knox.
 - (9) Aircraft accident or incident (Class A, B, and C). Any type of aircraft accident or incident that causes damage to aircraft or injury to personnel (manned or unmanned). Reporting requirements extend to tenant or transient aircraft from another service or command using Fort Knox facilities or land in the Fort Knox AOR.
 - (10) Command, control, communications, and computers (C4) outages. Report planned and unplanned degradations of C4 capabilities. A reportable degradation is:
 - (a) The loss of 50 percent or greater of a specific communications capability of e-mail, Nonsecure Internet Protocol Router Network (NIPRNET) service, or Secret Internet Protocol Router Network (SIPRNET) service.
 - (b) Any degradation that results in a significant negative impact on the ability of the commander to exercise command and control.
 - (11) Suspected or confirmed information system incidents or intrusions. Incidents or events to be reported are defined in AR 25-2, para 4-21.
 - (12) PII breaches/Loss. This applies to all Soldiers (and Cadets), civilian personnel assigned, attached, detailed, or on temporary duty with Fort Knox organizations that

control or collect PII. Include a copy of the completed Department of Defense (DD) Form 2959 with the SIR report. Report using procedures in Appendix C.

(13) Man-made or natural incident that impact on operations and training.

(a) Any major crisis resulting in disruption to installation operations, electrical outage, loss of water, sewage, heating, communications, cooling capabilities that effect quality of life (QOL) or damages/destruction to the installation including Soldier Family Assistance Center, Child Development Center/Child Youth School Services facility, barracks, chapels or billeting issues.

(b) Impact of imminent or forecasted natural or manmade disaster impacting unit operations, for example: tsunami warning, earthquake, hurricane warnings, flooding, winter weather (causing closure or delay), major brush or wild fires.

(c) Environmental incident or action that shuts down unit operations or training including spills, range fires, legal suits, administrative order that would stop operations, or an environmental incident requiring immediate notification to any Department of Defense (DoD) or external agency.

(d) That result in evacuation of facilities, or potential severe degradation of the environment. Examples include spills of petroleum, oil, and lubrication products into storm drains or waterways; release of substances such as chlorine gas and other hazardous substances in reportable quantities or greater, as defined in Federal, state, and local regulations; or when effects cause illness to the exposed individual(s).

(e) Serious or catastrophic failure to an operating system at a facility that has been licensed by a state or Federal regulatory agency (for example, sewage treatment plant, drinking water treatment plant, hazardous waste treatment or storage facility, etc.). Particularly, if provisions in the permit and/or governing regulations require timely reporting to the regulatory agency with oversight authority, and it is reasonable to expect an enforcement action will follow. Notices of violations require coordination with Army legal counsel. (See AR 200-1, para 2-3, for notices of violation.)

(14) Report reduced funding resulting in potential negative impact on Life, Health, Protection and Safety programs, Civilian hires, Contracts, Grants, Operation, Construction, Facilities, Soldier and Family Support.

(15) Trainee abuse or hazing and misconduct by platoon sergeant, drill sergeant, recruiter, ROTC/Junior ROTC (JROTC) cadre and/or cadet.

(a) Allegations of trainee abuse as defined in TRADOC Regulation 350-6, (any improper or unlawful physical, verbal, or sexual act against a trainee; or acts involving a trainee against trainee). Trainee abuse, platoon sergeant and drill sergeant misconduct will be reported in accordance with TRADOC Regulation 350-6.

(b) Allegations of platoon and drill sergeant misconduct not related to trainee abuse.

(c) Allegations of Recruiter and ROTC/JROTC Cadre misconduct while in a training status.

(16) Bomb threats on Fort Knox, as well as ROTC brigades, battalions, companies, and detachments.

(17) Radiological event. A radiological event encompassing radiological material accidents, incidents, and other circumstances where there is a confirmed or potential release to the environment, exposure of personnel above established limits, threat to the security of radiological material (including loss or theft), or any event of concern to the SC.

(18) Incidents/accidents involving international students and personnel with duty in a foreign country. Reportable incidents/accidents include absent without leave (AWOL), disciplinary problems, any training accident, or any accident causing injury or death.

(19) Report anytime a military or garrison support entity is dispatched off post to assist civilian authorities under any agreement or regulatory requirement (appendix E).

(20) Any incident involving spillage of classified information.

(21) Suspicious activity (appendix D).

(22) Any incident occurring in a CYS Services program or facility that include:

(a) Injury to a child/youth sustained on a CYS Services program or facility that result in admission to a hospital or which prevents/precludes the child/youth from participating in school/child development center (CDC) Youth programs for more than three (3) days.

(b) Child neglect or physical or sexual abuse allegations resulting in arrest of any person working or volunteering in any CYS Services program, even if the allegations did not involve a child enrolled in a CYS Services program.

(c) Any substantiated child neglect or abuse charge.

(d) Revocation or deferment of accreditation for any CDC or School age Center.

(e) Note: There are special CDC/CYSS reporting requirements in the IMCOM Commanders CCIR.

(24) Significant very important person (VIP) visits. Any visit by the Secretary of the Army (SECARMY), Chief of Staff of the Army (CSA), Vice Chief of Staff of the Army (VCSA), Sergeant Major of the Army (SMA), the Assistant Secretary of the Army (IE&E), and all 3 star or 3 star equivalent and above personnel; or elected /appointed government officials. This does not include those personnel who are here for Army boards and other activities whose visit may be classified or close hold.

(25) Any serious incident/misconduct involving a senior leader (Master Sergeant, field grade officer, GS-15 and above).

(26) Any other incidents not specifically covered in this regulation that the commander determines to be of concern to the Senior Commander or HQDA based on the nature, gravity, potential for adverse publicity, or potential consequences of the incident.

(27) Any potentially adverse public affairs issue on the Installation that may affect the SC mission or the ability to provide services to the Community.

Chapter 3

Reporting Procedures

3-1. General

a. The incident reporting process ensures critical information is disseminated in a timely manner with accurately and identifies responsibilities and requirements for notification. The appropriate report is considered sensitive in nature and should be close hold and distributed only to those personnel with a valid need to know. The reports usually contain PII, dissemination of these reports will be by FOUO means, to include Public Key Infrastructure (PKI)/digitally signed and encrypted e-mail traffic.

b. The IOC is the only authorized reporting element for USACC and US Army

(1) If the IOC is the initial point of notification, provide all details to the appropriate commander for report processing. Approval authority for the information and content of the report is the director or tenant commander.

(2) **Incidents Involving Allegations of Rape or Sexual Assault.** There are significant privacy issues that must be adhered to involving rape or sexual assault IAW AR 600-20. Restricted reports will not be reported through incident reporting channels. The unrestricted reports sent to any e-mail distribution list **must not** include any victim PII in the report: the victim's name, age (say only adult or minor), social security number (SSN), or other details; the report should be as obscure as possible when describing the victim. Normal distribution lists for incident reports may include those who do not need to know the victim's information for rape or sexual assault cases. Release the victim's name **ONLY** verbally to commanders and staff with the specific need to know. Family Advocacy and Army Community Service (ACS), Sexual Assault Response Coordinator (SARC)/Sexual Harassment/Assault Response Prevention (SHARP) Specialist, Victim Advocate (VA)/ SHARP Specialist or healthcare provider will be informed as appropriate. If the victim is a civilian or minor, only CID may release victim information. Include the DSAID report number in the report.

b. Submit a written report by email to the IOC as soon as possible, but no later than 1 hour, after the incident if there is a loss of weapon, life, limb, or eyesight or no later than 2 hours for other incidents – rapid (even if incomplete) initial reporting is preferred. Note: Mandatory timelines for SC reporting to DA, TRADOC, and IMCOM mirror these times.

(1) Use the EXSUM format (figure 3-2) for email body.

(2) Attach a detailed report (figure 3-3) to the email with the format below. (Partners use format as prescribed by higher HQs but ensure the same level of detail is provided.)

(3) Ensure the email is digitally signed and encrypted if PII is included.

Subject line: (Type Incident, unit/organization, ACOM of victim/subject, date of report, initial/follow-up/final)

Incident Report EXSUM

1. Unit and ACOM: (Company, Battalion, ACOM or command, ACOM)

2. What: (Reason for Report)

3. Who: (Name and Rank)

4. Where: (Specific Location)

5. When: (Specific incident time – DD HOUR MMM YY)

6. Any other HQ's notified: (Any headquarters off Fort Knox also notified)

7. Summary of Incident: (Detailed summary with condition, prognosis, etcetera)

POC for this report and requests for additional information (rank, name, title/position, phone, email):

Figure 3-2. Email EXSUM Format

FOR OFFICIAL USE ONLY (when filled in)
Detailed SIR Report Format

From:

To: CDRUSACC and FT Knox KY//IMKN-PL-IOC //

1. Report Date & Time: *(DD HOUR MMM YY)*
 2. Reporting Unit/Organization: *(Company, Battalion, ACOM or command, ACOM)*
 3. SIR#: *(enter unit report number if used)*
 4. Subject: *(Key word summary of type report – for example, SIR Serious Injury)*
 5. Status of Report: *(Initial, Follow-up, Final)*
 6. Category: *(1, 2, 3 or CCIR)*
 - 7a. Type of Incident: *(Indicate type of offense or incident, such as suicide, murder, or undermined death. If multiple offenses are involved, list in paragraphs below with most serious first.)*
 - 7b. Incident Sub-Cat 1: *(multiple offense 1)*
 - 7c. Incident Sub-Cat 2: *(multiple offense 2)*
 8. Date & Time of Incident: *(DD-HOUR-MMM-YY)*
 9. Location of Incident: *(Enter specific type of structure, facility, or area and exact address or location where the incident occurred; for example, on-post, off-post, barracks, hospital ward, arms room, building number, open field, housing address, etc.)*
 10. Summary of Incident: *(Provide detailed summary, to include specifics of outside agencies involved such as, local police, casualty assistance, Military Police, hospitals, SARC, etc.)*
 11. Racial: *(Yes or No)*
 12. Trainee Involvement: *(Yes or No)*
 13. DSAID Number: *(enter number or unknown)*
 - 14a. Name of Subject Involved: *(last, first, MI) [NOTE: the information in para 14 a-k is required for each subject]*
 - 14b. Subject's Rank/Title: *(For military, enter proper abbreviation of rank, for civilian employees, enter category and grade. For example, "WG6", "GS10", etc., and for other civilians, including Family members, enter "civilian".)*
 - 14c(1). Subject's ACOM: *(IMCOM, TRADOC, FORSCOM, AMRG, etc.)*
 - 14c(2). Subject's Component: *(Active, U.S. Army Reserves, Army National Guard, Other)*
 - 14c(3). Subject's Service: *(Army, Marines, Navy, Air Force, Coast Guard, or N/A)*
 - 14d. Subject's SSN#: *(last FOUR only)*
 - 14e. Subject's Race: *(American Indian/Alaskan, Asian, Pacific Islander, Black, White, Hispanic, Multi-Racial)*
 - 14f. Subject's Sex: *(M or F)*
 - 14g. Subject's Age: *(##)*
 - 14h. Subject's Position: *(If military, enter duty assignment, if Civilian employee, enter job title; if Family member, enter relationship to sponsor, for example: Family member- Spouse. For other civilians, enter occupation)*
 - 14i. Subject's Security Clearance: *(Secret, S-NAC, TS, Interim, None, etc.)*
 - 14j. Subject's Unit & Station: *(Enter unit and station of assignment: if military enter the unit designation and address; if Civilian employee, enter the organization name and address; if Family member, enter the rank, name and unit of the sponsor followed by the home address; if other civilian, enter home address)*
 - 14k. Subject's Duty Status: *(If military: on duty, leave, TDY, AWOL, Hospital, confinement, Cadet, Trainee, etc.; for civilian employees: on duty, off duty; for other civilians, to include Family members: N/A)*
 - 15a. Name of Victim: *(See para 14a explanation above)*
- Note: The information in para 15(a-k) is required for each victim.*

Figure 3-3. Detailed SIR Report Format

-
- 15b. Victim's Rank/Title: *(See para 14b explanation above)*
 - 15c(1). Victim's ACOM: *(See 14c explanation above)*
 - 15c(2). Victim's Component: *(See 14c explanation above)*
 - 15c(3). Victim's Service: *(See 14c explanation above)*
 - 15d. Victim's SSN#: *(See 14d explanation above)*
 - 15e. Victim's Race: *(See 14e explanation above)*
 - 15f. Victim's Sex: *(See 14f explanation above)*
 - 15g. Victim's Age: *(##)*
 - 15h. Victim's Position: *(See 14h explanation above)*
 - 15i. Victim's Security Clearance: *(See 14i explanation above)*
 - 15j. Victim's Unit & Station: *(See 14j explanation above)*
 - 15k. Victim's Duty Status: *(See 14k explanation above)*
 - 16. NOK Notification: *(For deaths and life threatening injuries only; state is NOK has been notified: Yes or No, specific time, by whom)*
 - 17. Soldier Deployed within Last Year?: *(Yes or No indicate if either subject and/or victim was deployed and dates; for example: Subject Yes, Jan 13 to Nov 13)*
 - 18. Were Seatbelts Worn? *(Yes, No, or N/A)*
 - 19. Was Alcohol Involved? *(Yes, No, or N/A)*
 - 20. Was PPG/E Worn? *(Motorcycle Accidents only – Yes, No, or N/A)*
 - 21. Any Previous Medical History? *(If medical history relates to this incident – Yes, No, or N/A)*
 - 22. Were Combat Lifesavers Present? *(For Deaths only - Yes, No, or N/A)*
 - 23a. Was CPR Performed at the Scene? *(For Deaths only - Yes, No, or N/A)*
 - 23b. Date & Time CPR Started: *(For Deaths only)*
 - 23c. Date & Time 911 Called: *(For Deaths only)*
 - 23d. Date & Time EMS Personnel Arrived on Scene: *(For Deaths only)*
 - 23e. Date & Time EMS Departed Scene En Route To Hospital: *(For Deaths only)*
 - 23f. Date & Time EMS Arrived at Hospital: *(For Deaths only)*
 - 23g. Date & Time Soldier Pronounced Dead: *(For Deaths only and who pronounced)*
 - 24a. Was anything different noticed about the Soldiers performance: *(Yes, No, or N/A)*
 - 24b. If yes, please explain: *(Describe actions that may have been a precursor to this incident)*
 - 25. Ages/Gender of Family members: *(For Deaths only)*
 - 26a. Type of Training: *(If pertinent to the incident)*
 - 26b. Phase of Training: *(If pertinent to the incident)*
 - 27. Weather Conditions at Time of Incident: *(If pertinent to the incident)*
 - 28. Other Factors Contributing to the Incident:
 - 29. Publicity: *(Local and social media with links to articles)*
 - 30. Commander Reporting: *(Rank, Name, Title/position, Unit, phone number, email address)*
 - 31. Point of Contact: *(Rank, Name, Title/position, unit/organization, phone number, email address).*
 - 32. Comments/Remarks: *(Include links to media coverage or additional information)*
 - 33. Downgrading Instructions: FOUO protective markings will not be removed as this contains personally identifiable information.

FOR OFFICIAL USE ONLY (when filled in)

Figure 3-3. Detailed SIR Report Format (continued)

3-3. Commanding General's (CG's) Update Requirements

- a. These updates are required for these categories of personnel:
 - (1) Soldiers assigned to Fort Knox.
 - (2) DA Civilians and Family members when the incident occurs on the installation.
 - (3) Other personnel as directed.
- b. The loss of life, limb or eyesight require the CG's Update report.

c. The victim's commander will submit a CG's Update (figures 3-4 (email) and 3-5 (attachment)) to the IOC between 12 and 24 hours but not later than 24 hours, after the initial report. The IOC will assist with coordination and collation of information from all agencies listed in the detailed report.

- (1) Ensure the report is digitally signed and encrypted.
- (2) Provide follow-up reports NLT 0900 daily until directed by the SC.

CG's Update Email EXSUM:

1. Name/phone number of person sending report: (Rank, Name, Title/Position, Unit/Organization, phone, email)
2. Changes in circumstances, errors, or information not included in the original report/since last update: *(Describe)*
3. Outstanding issues/coordination necessary: *(Describe)*
4. Any other information deemed necessary by the commander: *(Describe)*

Figure 3-4. CG's Update Email EXSUM

FOR OFFICIAL USE ONLY (when filled in)
Commanding General's Update

Fort Knox Incident Report #: *(As provided by the IOC)*

DTG of Update:

Subject(s) and/or Victim(s) and Unit(s):

Brief recap of incident:

1. Victim Commander's Report:

- a. Name/phone number of person sending report: *(Rank, name, title/position, Unit, phone number, email address)*
- b. Any significant ongoing actions associated with the incident: *(Describe)*
- c. Changes in circumstances, errors, or information not included in the original report: *(Describe)*
- d. If serious injury, any change in the condition or location of the injured or what is the prognosis: *(Describe)*
- e. If death, provide detailed NOK information *(who is the person survived by – names/ages/relationship/location/ mailing address, phone number for commander letters of condolence):*
- f. Memorial service location/DTG and unit attendees: *(Specific details)*
- g. Any other information deemed necessary by the commander: *(Describe)*

2. DHR Report, CAC (Casualty Assistance Center):

- a. Name/phone number of person sending report: *(Rank, name, title/position, Unit, phone number, email address)*
- b. Confirmation of DA Casualty Report: *(DTG of report)*
- c. Location/disposition of remains: *(location of remains and/status)*
- d. Names/ages/relationship of next of kin: *(Full name/age/relationship to deceased)*
- e. Status of next of kin notification: *(when, where, and by whom was the notification made)*
- f. Status of appointment of Casualty Assistance Officer: *(who, when appointed)*
- g. Burial honors: *(unit to conduct, date contacted)*
- h. Any other information deemed necessary: *(Describe)*

3. MEDDAC Commander's Report:

- a. Name/phone number of person sending report: *(Rank, name, title/position, Unit, phone number, email address)*
- b. Condition and prognosis of the patient: *(Describe as allowed by HIPAA communication within command channels)*
- c. Any existing conditions that may cause illness/injury to other personnel: *(Describe)*

Figure 3-5. CGs Update Report

-
- d. Any preliminary causes of death or autopsy results that are pertinent: *(Describe)*
 - e. Any other information deemed necessary: *(Describe)*
- 4. Provost Marshal's Report:**
- a. Name/phone number of person sending report: *(Rank, name, title/position, Unit, phone number, email address)*
 - b. Status of ongoing or planned investigation: *(Describe)*
 - c. Preliminary findings of investigation: *(Describe as allowed for command reporting)*
 - d. Any other information deemed necessary: *(Describe)*
- 5. Public Affairs Officer Report:**
- a. Name/phone number of person sending report: *(Rank, name, title/position, Unit, phone number, email address)*
 - b. Status of press releases: *(Describe)*
 - c. Any impacts of public opinion or routine operations pertaining to the SIR: *(Describe)*
 - d. Any other information deemed necessary: *(Describe)*
- 6. Safety Director Report:**
- a. Name/phone number of person sending report: *(Rank, name, title/position, Unit, phone number, email address)*
 - b. Any safety-related issues pertaining to the incident: *(Describe)*
 - c. Recommendations to mitigate safety risks associated with the incident: *(Describe)*
 - d. Any other information deemed necessary: *(Describe)*
- 7. Information compiled by:** *(Name, rank/position, unit/organization, duty position, phone number)*

FOR OFFICIAL USE ONLY (when filled in)

Figure 3-5. CGs Update Report (continued)

Appendix A References

Section I Required Publications

ALARACT 014-2012, (CORRECTED COPY)

HQDA CCIR EXORD 034-12 MOD 01 - Senior Leader Critical Command Information Requirements (HQDA CCIR Listing)

ALARACT 175/2013

Subject: MOD 1 To Compliance IAW DOD Directive 3025.18

AR 5-9

Area Support Responsibilities

AR 25-2

Information Assurance

AR 190-30

Military Police Investigations

AR 190-45

Law Enforcement Reporting

AR 340-21

The Army Privacy Program

AR 385-10

The Army Safety Program

AR 600-8-1

Army Casualty Program

DA Pamphlet 600-24

Suicide Prevention and Psychological Autopsy

DOD 3025.18

Defense Support of Civil Authorities (DSCA)

DOD 5400.11-R

Department of Defense Privacy Program

FKICAN Incident Response Plan

NEC Policy 140618001

TRADOC Regulation 350-6

Enlisted Initial Entry Training (IET) Policies and Administration

TRADOC Regulation 385-2

TRADOC Safety Program

IMCOM Regulation 190-45-1

United States Army Installation Management Command (IMCOM) Serious Incident Reports (SIRs) (Commanders Critical Information Reports (CCIR))

U.S. Army Cadet Command Memo

Subject: Serious Incident Reports (SIRs), 2 DEC 2013

CCIR

As published by the CGs of TRADOC, IMCOM, FORSCOM, ARNORTH and other HQ orders.

Section II

Related Publications. A related publication is a source of additional information. The user does not have to read a related reference to understand this publication

AR 11-2

Management Control

AR 25-55

The Department of the Army Freedom of Information Act Program

AR 40-5

Preventive Medicine

AR 190-53

Interception of Wire and Oral Communications for Law Enforcement Purposes

AR 200-1

Environmental Protection and Enhancement

AR 360-1

Public Affairs

AR 380-13

Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

AR 381-10

U.S. Army Intelligence Activities

AR 420-1
Army Facilities Management

AR 600-20
Army Command Policy

AR 710-2
Supply Policy below the National Level

Comprehensive Drug Abuse Prevention and Control Act of 1970

Fort Knox Regulation 27-10
Military Justice

United States Code of Military Justice

Watch Officer Incident Reporting Procedures SOP

Section III
Prescribed Forms.

Except where otherwise indicated below, the following forms are available on the Army Publishing Directorate (APD) Web site.

DD Form 2959
Breach of Personally Identifiable Information (PII) Report

Section IV
Referenced Forms

DA Form 1045
Army Ideas for Excellence Program (AIEP) Proposal

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B Management Control Checklist

B-1. Function

The function covered by this checklist is the administration of incident reporting.

B-2. Purpose

The purpose of this checklist is to assist unit managers and management control administrators in evaluating the key management controls outlined below. It is not intended to cover all controls.

B-3. Instructions

Answers must be based on the actual testing of key management controls (for example, document analysis, direct observation, sampling, simulation, other). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years.

B-4. Test Questions

- a. Is the correct format used for SIRs?
- b. Are initial telephonic/e-mail notifications of SIR incidents reported to the appropriate HQs immediately upon discovery or notification at the installation level?
- c. Are initial written incident reports sent to the appropriate HQs and staff within 4 hours of initial discovery or notification at the installation level?
- d. Do initial SIRs contain all the relevant information (who, what, when, where, and why) available at the time?
- e. Are follow-up reports forwarded to the requesting HQs within 2 hours of the request for follow-up information?
- f. Are SIRs digitally signed and encrypted from the originator through all the intermediate approval levels to the appropriate HQs?
- g. Are SARs used in accordance with appendix D of this regulation?
- h. Are SARs submitted to the IMCOM, TRADOC and DA within one hour of knowledge of the incident?
- i. Does the staff conduct trend analysis and provide feedback on identified trends to the leadership and Senior Commander on a routine basis?

B-5. Suppression

No previous management control evaluation checklist exists for this program

B-6. Comments

Make this a better tool for evaluating management controls. Submit comments directly to Directorate of Plans, Training, Mobilization, and Security (DPTMS) (IMKN-PLI-OC), Fort Knox, Kentucky 40121-5717.

Appendix C PII Reporting

C-1. Reporting Requirements

The loss of PII will be reported IAW Incident Response Plan for the Fort Knox Campus Area Network (currently in revision).

C-2. Initial Notifications

- a. Immediately notify the Fort Knox IOC at (502) 624-2707 and/or usarmy.knox.imcom-atlantic.mbx.ioc-watch-ofcr@mail.mil and specify impact category (High: greater than 500 individuals or Moderate: less than or equal to 500)
- b. Notify the United States Computer Emergency Readiness Team (US-CERT) at <http://www.us-cert.gov> within 1 hour of discovering the incident. Note: Internal and command notification must not delay the 1-hour US-CERT reporting.
- c. Immediately send an e-mail to piireporting@us.army.mil, including initially available information obtained on DD Form 2959 (Breach of Personally Identifiable Information (PII) Report) and provide a copy of the e-mail to usarmy.knox.93-sig-bde.list.nec-ia-office@mail.mil and usarmy.knox.imcom-atlantic.mbx.ioc-watch-ofcr@mail.mil.

C-3. Additional Notifications

- a. In addition to command and IOC telephonic notification, contact the Fort Knox Information System Support Manager at 502-624-7633 and seek additional guidance.
- b. Notify the unit/organization/command Freedom of Information Act (FOIA)/Privacy Act (PA) Officer.

C-4. Written Reporting

- a. Complete the formatted PII Incident Report and forward it to the HQDA Freedom of Information (FOIA)/Privacy Act (PA) Office within 24 hours of discovery of incident. The reporting format and submission guidelines are located at: <https://www.rmda.army.mil/privacy/RMDA-PO-Infractions.html>.
- b. Provide the IOC an incident report EXSUM on the incident. Attach copies of the PII Incident Report and the DD Form 2959 (Breach of Personally Identifiable Information (PII) Report).

C-5. Follow-on Actions

- a. Follow the procedures IAW Incident Response Plan for the Fort Knox Campus Area Network (currently in revision).
- b. Coordinate with the Staff Judge Advocate to send affected individuals the notification letter within 10 days. Notification should occur from a sufficient management level (Commander or CofS) to reassure impacted individuals of the seriousness of the event.
- c. Continue to update US-CERT and the IOC via e-mail and the PII reporting site, until the investigation is closed and all individuals have been notified.

Appendix D

Suspicious Activity Report (SAR) Reporting

D-1. General

Suspicious activity report (SAR) reporting is established to provide a means to capture all-threats and suspicious activity against all Fort Knox assets (figure D-1).

D-2. SAR Activities to report.

a. Acquisition of expertise. Unjustified attempts to obtain or conduct specialized training in security concepts, military weapons or tactics, or other unusual capabilities such as specialized transport or handling capabilities that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

b. Breach or attempted intrusion. Unauthorized entry or attempted entry into a restricted area or protected site; impersonation of authorized personnel (for example, police, security, or janitorial personnel).

c. Eliciting information for an unlawful purpose. Suspicious questioning of personnel by any means about particular DoD structures, functions, personnel, or procedures at the facility or infrastructure.

d. Expressed or implied threat. A threat to DoD personnel or threatened damage to or compromise of a DoD facility or infrastructure.

e. Flyover and/or landing. Suspicious overflight of and/or landing near a DoD facility or infrastructure by any type of flying vehicle (for example, airplane, helicopter, unmanned aerial vehicle, hang glider).

f. Materials acquisition and/or storage. Acquisition of unusual quantities of precursor material (for example, cell phones, pagers, fuel, and timers); unauthorized or unlicensed individual or group attempts to obtain precursor chemicals, agents, or toxic materials; and/or rental of storage units for the purpose of storing precursor material, chemicals, or apparatuses for mixing chemicals.

g. Misrepresentation. Misusing or presenting false insignia, documents, or identification or engaging in any other activity to misrepresent one's affiliation.

h. Recruiting. Building operations teams and contacts, personnel data, banking data, or travel data under circumstances that would cause a reasonable person to perceive a threat to DOD personnel, facilities, or forces in transit.

i. Sabotage, tampering, and/or vandalism. Damaging, manipulating, or defacing part of a DoD facility, infrastructure, or protected site. Acts of vandalism committed by DoD civilian employees, Service members, or their dependents should not be reported as suspicious activity unless those acts relate to a pattern of criminal activity or otherwise would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

j. Surveillance. Monitoring the activity of DoD personnel, facilities, processes, or systems including showing unusual interest in a facility, infrastructure, or personnel (for example, observation through binoculars, taking notes, drawing maps or diagrams of the facility, and taking pictures or video of a facility, infrastructure, personnel, or the surrounding environment) under circumstances that would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

k. Testing of security. Interactions with or challenges to DoD installations, vessels, personnel, or systems that could reveal physical, personnel, or cyber security capabilities including attempts to compromise or disrupt DoD information technology infrastructures.

l. Theft, loss, and/or diversion. Theft or loss associated with a DoD facility or infrastructure (for example, badges, uniforms, identification cards, emergency vehicles, technology, or documents whether classified or unclassified) that are proprietary to the facility, and/or a diversion of attention from a DoD facility or infrastructure that is related to a theft or loss associated with that facility.

m. Weapons discovery. Discovery of weapons or explosives. The discovery of personal weapons legally owned by DoD civilian employees, Service members, or their dependents should not be reported as suspicious activity if the discovery is solely the result of the owner's failure to properly store or secure the weapons.

n. Unexplained Absences of International Military Students. International military students who are unexpectedly absent from scheduled activities when the absence is without proper authorization and lasts more than 24 hours, and an appropriate official with the host DoD organization determines that the absence is not due to a misunderstanding in scheduling, to sickness, or to another similar reason.

D-3. Procedures

a. Report suspicious activity to the offices below for evaluation and entry into eGuardian, if the incident meets eGuardian criteria:

(1) Unit Antiterrorism (AT) Officer. The unit AT Officer will report the incident to the Fort Knox AT Officer at 502-624-7578.

(2) DES at 502-624-2111

(3) Fort Knox 902nd Military Intelligence (MI) office at 502-624-3991.

(4) Fort Knox IOC using the format below.

b. Use the report format in figures D-1 and D-2.

Email Subject: *(SAR Report, Unit/Organization, Date)*

SAR Incident Report EXSUM

Summary: (answer the who, what, when, where, why and how):

1. Initial response or action taken: *(Describe what specific actions taken)*
2. Indication of whether the incident is open or closed/resolved/unresolved: *(Describe status of incident)*
3. Source and assessment of credibility of the source: *(Describe where the information came from)*
4. Coordinating agencies (local law enforcement, FBI, 902nd MI, etc.): *(Identify agency you contacted)*

POC: *(rank, Name, Title/position, unit/organization, phone number, email address)*

Note: A follow-up report will be submitted after the final determination has been made.

Figure D-1. SAR Email EXSUM Format

SUSPICIOUS ACTIVITY REPORT (SAR)

1. **SAR NUMBER:** XX-001 (*For example, the XX would be the last two numbers of the calendar year.*)
2. **CLASSIFICATION:** (U/FOUO/LES)
3. **REPORTING DATE/TIME:** (DD MMM YY/0000)
4. **REPORTING UNIT/ORGANIZATION:** (*Unit/Organization/Activity and location*)
5. **INCIDENT DATE/TIME:** DD MMM YY/0000 (*If unknown state "unknown".*)
6. **INCIDENT TYPE:** (*Nonspecific threat/surveillance/elicitation/tests of security/intrusions/repetitive activities/suspicious activities/incidents*)
 - 6a. **Nonspecific threat.** *A nonspecific threat received by any means, which contains a specific time, location, or area for an attack against U.S. forces, facilities, or missions. This includes, but is not limited to, any event or incident, or series of events or incidents, which in and of themselves may indicate the potential for a threat to U.S. forces, facilities, or mission, regardless of whether the threat posed is deliberately targeted or collateral (that is, demonstrations).*
 - 6b. **Surveillance.** *Any reported possible surveillance in which an attempt to record information or to use unusual means to monitor activities is observed. Such attempts may include use of cameras (still or video), note taking, annotated maps or drawings, any reports from host nation security forces of possible surveillance of U.S. assets.*
 - 6c. **Elicitation.** *Any attempt to obtain security related or military specific information by anyone who does not have the appropriate security clearance and the "need to know." Elicitation attempts may be made by mail, fax, telephone, computer, or in person.*
 - 6d. **Tests of security and intrusions (attempted or successful).** *Any attempt to measure security reaction times or strengths; any attempts to test or to penetrate physical security barriers or procedures; any attempts to acquire or duplicate uniforms, badges, passes, or other security related documents.*
 - 6e. **Repetitive activities.** *Any activity that meets one of the other criteria listed in this paragraph and has occurred two or more times in the same location by the same person and/or vehicle, within a 1 month period.*
 - 6f. **Suspicious activities/incidents.** *This category should ONLY be used if the reportable information DOES NOT meet any of the above criteria. Any activity/incident that does not specifically fit into the aforementioned five categories yet is believed to represent a force protection threat should be reported under this category. Examples of this include: incidents resulting in the scrambling of homeland defense assets; thefts of material that could be used to manufacture false identification cards; thefts of military uniforms which may be used to gain access to a military installation, vandalism, etc.*
7. **STATUS:** (*open/resolved; open/unresolved; closed/resolved; closed/unresolved.*)
8. **SYNOPSIS:** (*One sentence description of incident, for example, possible photograph of front entrance to Chaffee Gate, Fort Knox, KY.*)
9. **FACTS OF INCIDENT:** (*Answer the questions who, what, when, where, why and how? For example, at 1300, 10 Sep 07, Smith was conducting surveillance of the Gate using binoculars and a video camera. Smith was apprehended by the MPs and interviewed. Smith stated the video was to be used for plotting an attack against Ft. Patton.*)
10. **PERSON(S) BRIEFED:** (*For example, COL Jones, Cdr, 4th ESC on DD-MMM-YY.*)

Figure D-2. Detailed Report Format

Appendix E

Defense Support to Civil Authorities

E-1. Applicability.

Report anytime a military or garrison support entity is dispatched off post to assist civilian authorities under any agreement or regulatory requirement. This also includes immediate response provided by the installation commander under the provisions of Department of Defense Directive (DoDD) 3025.18, Defense Support of Civil Authorities (DSCA) in order to save lives, prevent human suffering, or mitigate great property damage. Use the report format in figure E-1.

- a. This reporting requirement DOES NOT apply to fire and emergency services actions taken in support of memorandum of agreements (MOA), mutual aid agreements (MAA), etcetera.
- b. This reporting requirement DOES apply to explosive ordnance and/or military working dog requests in support of AR 5-8, Area Support Requirements, unless covered in formal MOAs, MAAs, etc.
- c. Routine DSCA (not covered by agreement (MOA, MAA, etc.) requests require a legal review by the Fort Knox SJA for approval through the Department of the Army to the Secretary of Defense, per DoDD 3025.15.
- d. An immediate response shall end when the necessity giving rise to the response is no longer present (such as when there are sufficient resources available from State, local, and other Federal agencies to respond adequately and that agency or department has initiated response activities) or when the initiating Department of Defense (DoD) official or a higher authority directs an end to the response. The DoD official directing a response under immediate response authority shall reassess whether there remains a necessity for the Department of Defense to respond under this authority as soon as practicable but, if immediate response activities have not yet ended, not later than 72 hours after initiation.

E-2. Request Evaluation Criteria.

- a. All non-immediate response requests require a legal review by the SJA, Fort Knox before approval. The CG, USACC is the only Fort Knox DoD official who can direct the response under immediate response authority.
- b. Requests (if not already addressed in a MOAs, MOAAs, etc.) from civil authorities and qualifying entities for assistance shall be evaluated for:
 - (1) Legality (compliance with laws).
 - (2) Lethality (potential use of lethal force by or against DoD Forces).
 - (3) Risk (safety of DoD Forces).
 - (4) Cost (including the source of funding and the effect on the DoD budget).
 - (5) Appropriateness (whether providing the requested support is in the interest of the Department).
 - (6) Readiness (impact on the DoD's ability to perform its other primary missions).

E-3. Requirements for Reporting.

When operational (MTO&E/non-garrison) resources are used in an immediate response role, no later than 2 hours after the response is initiated, the IOC must report the

request. The CG, USACC is the only Fort Knox DoD official to direct the response under immediate response authority. Reports will be made to the following agencies with (cc: to IMCOM and TRADOC).

a. The Army Operations Center (AOC) can be contacted at: (NIPR) USARMY.PENTAGON.HQDA.MBX.AOC-TEAM-CHIEF-ARMY-G3@MAIL.MIL; (SIPR) USARMY.PENTAGON.HQDA.MBX.AOC-TEAM-CHIEF-ARMY-G3@MAIL.SMIL.MIL; commercial 703-695-0575; 703-695-4695; DSN 312-225-0575;312-225-4695.

b. The Army Domestic Support Division (DOMS) can be contacted At: (NIPR) USARMY.PENTAGON.HQDA-DSC-G-3-5-7.MBX.DOMS-TEAM-CHIEF-ARMY-G3@MAIL.MIL; (SIPR) USARMY.PENTAGON.HQDA-DSC-G-3-5-7.MBX.DOMS-TEAM-CHIEF-ARMY-G3@MAIL.SMIL.MIL; commercial 703-695-2679; DSN 312-225-2679.

E-3. Timeline for Reporting.

- a. The initial report of the request will be submitted within 2 hours to the IOC.
- b. A final report is required upon mission complete.

SUBJECT: DA SIR CAT 3, DSCA, unit/organization, ACOM, date of report, initial/follow-up/final

DSCA Incident Report EXSUM:

1. Unit and MACOM: *(for example - 4th ESC, FORSCOM)*
2. What: *(Reason for Report)*
3. Who: *(Name and Rank)*
4. Where: *(Specific Location)*
5. When: *(DD-HHH-MMM-YY)*
6. Any other HQ's notified: *(Identify any other organization off Fort Knox who is aware)*
7. Summary of Incident: *(Describe in detail)*
 - a. Situation requiring assistance: *(e.g., to save lives, prevent human suffering, mitigate property damage, etc.)*
 - b. Civil Authority requesting support: *(specific organization)*
 - c. Resources used in the response: *(specific equipment, training, supplies, etcetera)*
 - d. Time of response: *(DD-HHH-MMM-YY)*
 - e. Estimation of duration of response support: *(anticipated length of support)*
 - f. Impact to operations and/or training: *(anticipated or any impact on required operations or training)*
 - g. Other pertinent information: *(provide additional information not included above)*
8. POC for the report and requests for additional information: *(Name, rank/position, unit/organization, duty position, phone number)*

Figure E-1. DSCA Report Format

Appendix F AR 190-45 and AR 600-8-1 Reporting Areas of Responsibility

F-1. Fort Knox Area of Responsibility for reporting SIR's

The SC Fort Knox, CG, USACC is responsible for reporting incidents in these counties:

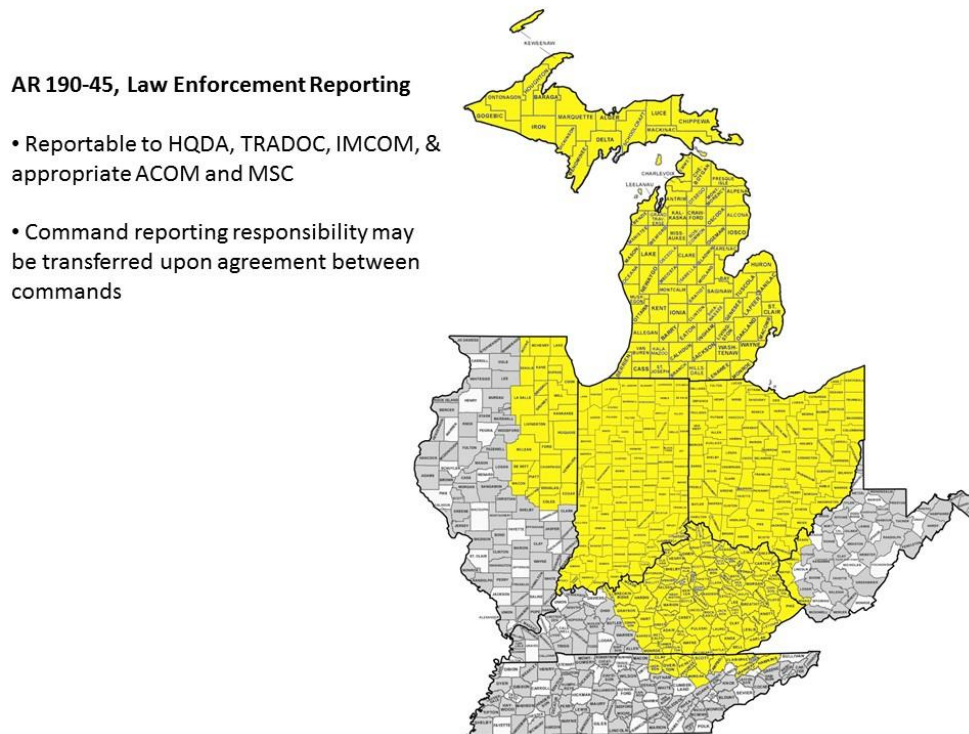


Figure F-1. AR 190-40 Fort Knox SIR Area of Responsibility

a. Illinois counties: Boone, Champaign, Coles, Cook, DeKalb, DeWitt, Douglas, Dupage, Edgar, Ford, Grundy, Iroquois, Kanakee, Kane, Kendall, Lake, LaSalle, Livingston, Macon, McHenry, McLean, Moultrie, Piatt, Vermillion, and Will.

b. Indiana counties: Entire state.

c. Kentucky counties: Adair, Anderson, Barren, Bath, Bell, Boone, Bourbon, Boyd, Boyle, Bracken, Breathitt, Breckinridge, Bullitt, Campbell, Carroll, Carter, Casey, Clark, Clay, Clinton, Cumberland, Edmonson, Elliott, Estill, Fayette, Fleming, Floyd, Franklin, Gallatin, Garrard, Grant, Grayson, Green, Greenup, Hancock, Hardin, Harlan, Harrison, Hart, Henry, Jackson, Jefferson, Jessamine, Johnson, Kenton, Knott, Knox, LaRue, Laurel, Lawrence, Lee, Leslie, Letcher, Lewis, Lincoln, Madison, Magoffin, Marion, Martin, Mason, McCreary, Meade, Menifee, Mercer, Metcalfe, Monroe, Montgomery, Morgan, Nelson, Nicholas, Oldham, Owen, Owsley, Pendleton, Perry, Pike, Powell, Pulaski, Robertson, Rockcastle, Rowan, Russell, Scott, Shelby, Spencer, Taylor, Trimble, Washington, Wayne, Whitley, Wolfe, and Woodford.

d. Michigan counties: Entire state.

- e. Ohio counties: Adams, Allen, Ashland, Athens, Auglaize, Brown, Butler, Champaign, Clark, Clermont, Clinton, Crawford, Darke, Defiance, Delaware, Erie, Fairfield, Fayette, Franklin, Fulton, Gallia, Greene, Hamilton, Hancock, Hardin, Henry, Highland, Hocking, Huron, Jackson, Knox, Lake, Lawrence, Licking, Logan, Lucas, Madison, Marion, Meigs, Mercer, Miami, Montgomery, Morgan, Morrow, Muskingum, Ottawa, Paulding, Perry, Pickaway, Pike, Preble, Putnam, Richland, Ross, Sandusky, Scioto, Seneca, Shelby, Union, VanWert, Vinton, Warren, Washington, Williams, Wood, and Wyandot.
- f. Tennessee counties: Campbell, Claiborne, Clay, Fentress, Hancock, Hawkins, Jackson, Morgan, Overton, Pickett, and Scott.
- g. West Virginia counties: Cabell, Mason, Mingo, and Wayne.

F-2. AR 600-8-1 Fort Knox Casualty Area of Responsibility

DHR, Fort Knox CAC is responsible to provide support in these counties:

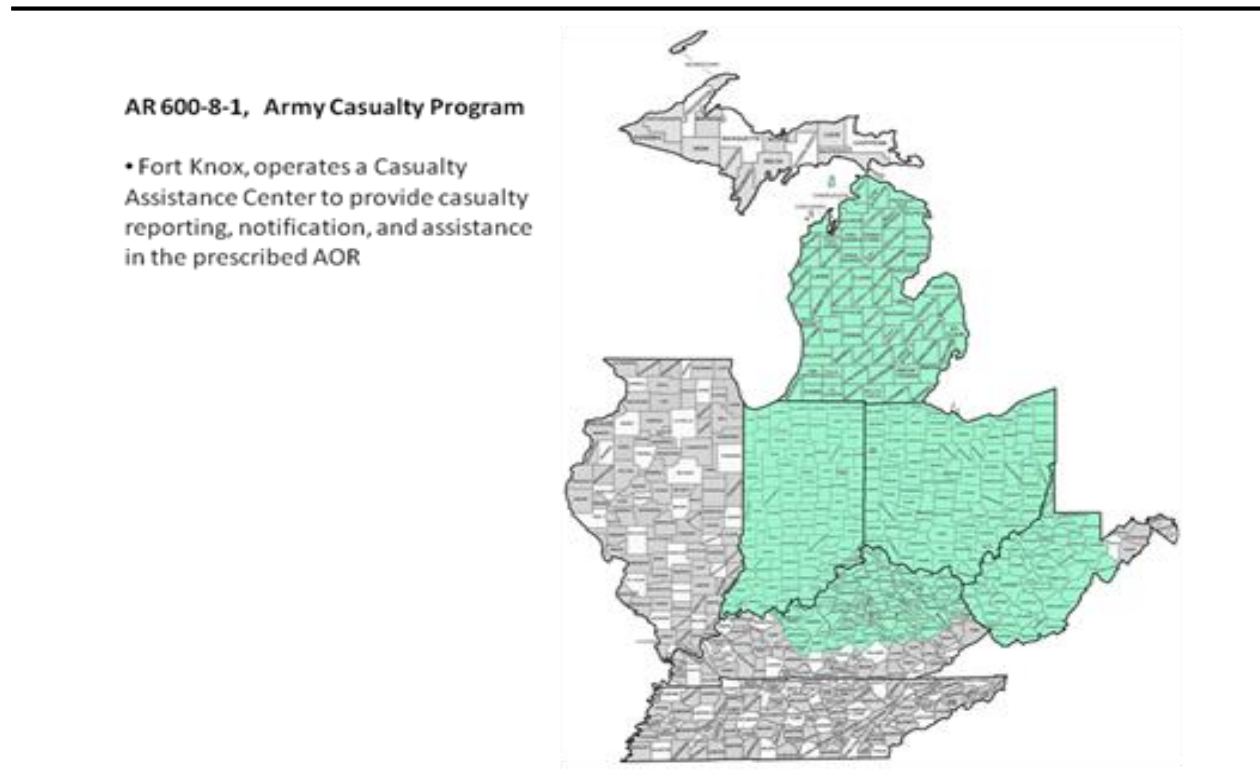


Figure F-2. AR 600-8-1 Fort Knox Casualty Area of Responsibility

- a. Kentucky counties: Anderson, Bath, Boone, Bourbon, Boyd, Boyle, Bracken, Breathitt, Breckinridge, Bullitt, Campbell, Carroll, Carter, Casey, Clark, Edmonson, Elliott, Estill, Fayette, Fleming, Franklin, Gallatin, Garrard, Grant, Grayson, Green, Greenup, Hancock, Hardin, Harrison, Hart, Henry, Jackson, Jefferson, Jessamine, Johnson, Kenton, LaRue, Lawrence, Lee, Lewis, Lincoln, Madison, Magoffin, Marion, Mason, Meade, Menifee, Mercer, Montgomery, Morgan, Nelson, Nicholas, Oldham, Owen, Owsley, Pendleton, Powell, Robertson, Rockcastle, Rowan, Scott, Shelby, Spencer, Taylor, Trimble, Washington, Wolfe, and Woodford.

b. Indiana counties: Entire state.

c. Ohio counties: Entire state.

d. West Virginia counties: Barbour, Boone, Braxton, Brooke, Cabell, Calhoun, Clay, Doddridge, Fayette, Gilmer, Greenbrier, Hancock, Harrison, Jackson, Kanawha, Lewis, Lincoln, Logan, Marion, Marshall, Mason, McDowell, Mercer, Mingo, Monongalia, Monroe, Nicholas, Ohio, Pendleton, Pleasants, Pocahontas, Preston, Putnam, Raleigh, Randolph, Ritchie, Roane, Summers, Taylor, Tucker, Tyler, Upshur, Wayne, Webster, Wetzel, Wirt, Wood, and Wyoming.

e. Wisconsin counties: Alcona, Allegan, Alpena, Antrim, Arenac, Barry, Bay, Benzie, Berrien, Branch, Calhoun, Cass, Charlevoix, Cheboygan, Clare, Clinton, Crawford, Eaton, Emmet, Genesee, Gladwin, Grand Traverse, Gratiot, Hillsdale, Huron, Ingham, Ionia, Iosco, Isabella, Jackson, Kalamazoo, Kalkaska, Kent, Lake, Lapeer, Leelanau, Lenawee, Livingston, Macomb, Manistee, Mason, Mecosta, Midland, Missaukee, Monroe, Montcalm, Montmorency, Muskegon, Newaygo, Oakland, Oceana, Ogemaw, Oselola, Oscoda, Otsego, Ottawa, Presque Isle, Roscommon, Saginaw, Sanilac, Shiawassee, St. Clair, St. Joseph, Tuscola, Van Buren, Washtenaw, Wayne, and Wexford.

Appendix G

DPTMS IOC- Watch Officer Procedures for Reporting

G-1. Watch Officer Actions

a. Comply with the procedures in this regulation and the “Watch Officer Incident Reporting Procedures” SOP upon notification of a reportable incident. (The SOP may be more up-to-date with changing guidance; this regulation may be in revision.)

b. Receipt. Upon receipt of an incident from a subordinate unit, obtain as much information as possible. Use the Incident Report Checklist and Notification Matrix at (figures G-1 and G-2) of this regulation as tools for actions. Provide the reporting unit/staff any assistance needed to properly and timely complete the report using the format, as required by the appropriate regulation.

c. Assessment/Notification. Use the SC CCIR matrix to determine if the incident is reportable. Verify reportability with the base regulatory guidance from DA, TRADOC, IMCOM, etc., before initiating the reporting process.

(1) If the incident is reportable, make the appropriate notification and begin reporting procedures.

(2) If the incident is determined not to be reportable or cannot be determined, but is of a serious nature, contact the SC CofS, GC, garrison manager, or DPTMS for further guidance.

d. Use the reporting flowchart (figure 3-1) as a guideline for notification and ensure that “who else needs to know” is considered for notification.

(1) Notify the CAC for all deaths and serious injuries.

(2) Notify the Safety Officer of all accident type incidents.

(3) Notify the IACH Plans, Training, Mobilization and Security (PTMS) Operations Officer for all medically related incidents.

e. Make initial telephonic report to TRADOC and IMCOM operations centers. Notify FORSCOM and ARNORTH for incidents as directed. The initial report of an incident will be reported as soon as possible. Optimally, reporting should be made within two hours after receiving the initial information and after authorization for release.

f. Approval authority for the information content of the report is the commander, director or tenant commander.

g. Brief the DPTMS or his/her designated representative on the information gathered and the intended report to higher headquarters.

h. Obtain approval for release of the telephonic and written reports:

(1) The USACC CofS is the approval authority for all TRADOC and DA SIRs

(2) The GC is the approval authority for all IMCOM SIRs and CCIRs.

i. Once approved, make an initial telephonic report. Ensure this report is annotated on the IOC log and incident checklist noting the date/time sent and name of the person who received the report.

j. Initiate written/electronic report.

(1) Begin applying the known information to the appropriate format.

(2) Provide a draft report to the release authority (above).

(3) Title the subject for all correspondence for the incident with: report number, and type incident, the headquarters of the Soldier, and date of incident, and status of report.

For example, DA SIR 15-0033, Death of a Soldier, 19th EN, FORSCOM, 13 MAR14, initial.

k. Submit written/electronic reports to the appropriate headquarters within two hours of notification of the incident and authorization for release, even if the information is incomplete. E-mail the report as an attachment, digitally signed and encrypted, using the appropriate e-mail distribution list. Ensure the e-mail body text contains an EXSUM. Verify receipt of the report and make the appropriate entry in the IOC duty log and Incident Report checklist with the date/time sent and name of the person verifying receipt. SIRs and OPREPS must also be reported using the TRADOC Reporting Portal.

l. Once approved distribute the report by email to the "ALL SIR" and "ALL SIR cc" distribution lists as well as the appropriate headquarters below (filter the distribution based on "need to know"). Once properly released, provide a courtesy copy of the report to IMCOM/IMCOM-AT and/or TRADOC emergency operations centers (EOC) if appropriate.

(1) DA SIR – submit to DA, courtesy copy to TRADOC (TRADOC Reporting Portal) and IMCOM/IMCOM-AT and to First Army (if First Army asset or mobilizing Soldier) or FORSCOM (if FORSCOM asset).

(2) TRADOC Incident/Soldier – submit to TRADOC (TRADOC Reporting Portal) and courtesy copy to IMCOM. Additionally, incidents involving ROTC cadre and cadets will be reported through their appropriate command to USACC who will forward to the IOC for reporting to TRADOC.

(3) IMCOM Incident – submit to IMCOM.

(4) FORSCOM Incident/Soldier – submit to FORSCOM, TRADOC (TRADOC Reporting Portal), and courtesy copy to IMCOM.

(5) Mobilizing Incident/Soldier – submit to First United States Army EOC with courtesy copies to IMCOM and TRADOC EOCs.

(6) Unit Training on Fort Knox – ensure unit submits report to its higher headquarters and provide courtesy copy TRADOC (TRADOC Reporting Portal) and IMCOM.

(7) WTU Soldier or cadre – submit to TRADOC (TRADOC Reporting Portal) and IMCOM.

(8) MEDDAC Incident/Soldier – submit to TRADOC (TRADOC Reporting Portal) and IMCOM.

(9) Any incident involving a garrison facility and/or garrison equipment or may impact on the garrison with publicity – submit to IMCOM.

m. Incidents Involving Allegations of Rape or Sexual Assault. Per AR 600-20, for any incident involving rape or sexual assault, there are significant privacy issues that must be adhered to. Restricted reports will not be reported through incident reporting channels. The report sent to any e-mail distribution list **must not** include any of the following information in the report: the victim's name, age (say only adult or minor), SSN, or other details; the report should be as obscure as possible when describing the victim. Normal distribution lists for incident reports may include those who do not need to know the victim's information for rape or sexual assault cases (CAC, Safety, etc.). Release the name on the report ONLY verbally to the command group. Family Advocacy and Army Community Service (ACS), Sexual Assault Response Coordinator (SARC)/Sexual Harassment/Assault Response Prevention (SHARP) Specialist, Victim

Advocate (VA)/ SHARP Specialist or healthcare provider will be informed as appropriate. If the victim is a civilian or minor, only the CID may release victim information. Include the DSAID report number in the report.

n. Follow-up Reports. Send follow-up reports to higher headquarters, as necessary, when additional information is obtained or the situation changes. Follow-up reports must be approved by the release authority prior to release.

o. Commanding General's Update. Assist the reporting commander in gathering and consolidating the following information within 12 to 24 hours, but not later than 24 hours, following the incident and forward to CofS, USACC, using the format figure 3-5:

p. The SC/CG, Fort Knox, has the responsibility to forward all SIRs that occur in the Fort Knox AR 190-45 area of responsibility, directly to HQDA and support casualty requirements within the AR 600-8-1 area of responsibility. The IOC will forward copies of SIRs directly to DA for all Fort Knox units and verify that tenant unit higher HQs send their SIR to DA.

Glossary

Section I Abbreviations

ACOM

Army command

AOR

area of responsibility

AR

Army regulation

ARNG

Army National Guard

ARNORTH

U.S. Army Northern Command

AWOL

absence without leave

CAC

Casualty Assistance Center

C4

command, control, communications, and computers

CCIR

commander's critical information requirements

CG

commanding general

CPR

cardiopulmonary resuscitation

COS

Chief of Staff

CYSS

Child Youth School Services

CCIR

Commanders' Critical Information Requirements

CDC

Child Development Center

CST

cadet summer training

CULP

Cultural Understanding & Language Proficiency

DA

Department of the Army

DCG

Deputy Commanding General

DCS

Deputy Chief of Staff

DD

Department of Defense

DES

Directorate of Emergency Services

DOD

Department of Defense

DRU

direct reporting unit

DSAID

Defense Sexual Assault Incident Database

DSN

Defense Switched Network

EMS

Emergency Medical Services

EXSUM

executive summary

FCC

Family Child Care

FOIA

Freedom of Information Act

FOUO

for official use only

FORSCOM

U.S. Army Forces Command

HQ

headquarters

HQDA

Headquarters, Department of the Army

HIPAA

Health Insurance Portability and Accountability Act

IMCOM

U.S. Installation Management Command

IMCOM-AT

U.S. Installation Management Command - Atlantic Region

IOC

installation operations center

MEDCOM

U.S. Army Medical Command

MI

military intelligence

MTF

medical treatment facility

MTO&E

modified table of organization and equipment

NAF

non-appropriated fund

NIPRNET

Nonsecure Internet Protocol Routing Network

OPS

Operations Center

OPREP

Operations Report

PII

personally identifiable information

PMO

Provost Marshall Office

POC

point of contact

ROTC

Reserve Officers' Training Corps

SAR

Suspicious Activity Report

SARC

sexual assault response coordinator

SC

senior commander

SIPR

Secure Internet Protocol Router Network

SIR

Serious Incident Reports

SFAC

Soldier Family Assistance Center

SSN

social security number

TRADOC

U.S. Army Training and Doctrine Command

UCMJ

Uniform Code of Military Justice

USACC

U.S. Army Cadet Command

USACIDC

U.S. Army Criminal Investigation Command

USAR

U.S. Army Reserve

US-CERT

United States Computer Emergency Readiness Team

WTU

Warrior Transition Unit

Section II**Terms****Bomb threats**

Communication by any means specifically threatening to use a bomb to attack against U.S. forces, facilities, or missions.

Category 1 serious incident

A serious incident that is of immediate concern to HQDA. Incidents that must be reported to HQDA as Category 1 serious incidents are listed in AR 190-45 chapter 8, paragraph 8-2.

Category 2 serious incident

A serious incident that is of concern to HQDA. Incidents that must be reported to HQDA as Category 2 serious incidents are listed in AR 190-45 chapter 8, paragraph 8-3.

Category 3 serious incident

An incident that is of concern to the IMCOM, ACOM, ASCC, or DRU (see AR 190-45 chapter 8 paragraph 8-4), any incident that must be reported to the IMCOM, ACOM, ASCC, or DRU as a category 3 serious incident according to an approved IMCOM, ACOM, ASCC, or DRU supplement to this regulation. Establishment of category 3 serious incidents is neither required nor reportable to HQDA.

Chemical agent

A chemical substance which is intended for use in military operations to kill, seriously injure, or incapacitate mainly through its physiological effects.

Controlled cryptographic items

Controlled cryptographic items are described as secure telecommunications or information handling equipment, associated cryptographic components, or other hardware items, which perform a critical communication security function.

Criminal investigation

An investigation of a criminal incident, offense, or allegation conducted by law enforcement personnel

Criminal offense

Any act or omission defined and prohibited as a criminal act by the UCMJ, the USC, state and local codes, foreign law, or international law or treaty. For juveniles, this term refers to acts which, if committed by an adult, would be subject to criminal penalties.

DSCA

Support provided by U.S. Federal military forces, DoD civilians, DoD contract personnel, DoD Component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected States, elects and requests to use those forces in title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events. Also known as civil support.

Family member

Includes those individuals for whom the Service member provides medical, financial, and logistical (for example, housing, food, and clothing) support. This includes, but is not limited to, the spouse, children under the age of 18, elderly adults, and persons with disabilities.

Hate crime

Crimes directed against persons, places of worship, organizations (and their establishments where individuals gather), because of their race, ethnic background, religious, or sexual orientation.

Hazing

Cruel, abusive, oppressive or harmful behavior that may or may not include physical, emotional or psychological acts and can occur at any function where Soldiers are present.

Juvenile

A subject of an incident who is under the age of 18, who was not a military member, spouse of a military member, or otherwise having been declared to have reached their majority at the time of an offense.

Next of kin

The person most closely related to the casualty is considered primary next of kin for casualty notification and assistance purposes. This is normally the spouse of married persons and the parents of single persons who have no children. The precedence of next of kin with equal relationships to the member is governed by seniority (age). The rights of minor children shall be exercised by their parents or legal guardian.

Personal information

Information about an individual that identifies, links, relates, or is unique to, or describes him or her, for example, a social security number (SSN); age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel; medical; and financial information, etc. Such information is also known as PII (that is, information which can be used to distinguish or trace an individual's identify such as their name, SSN, date and place of birth, mother's maiden name, and biometric records including any other personal information which is linked or linkable to a specified individual. This information can be in hard copy (paper copy files) or electronic format, stored on personal computers, laptops, and personal electronic devices such as Blackberries and found within databases. This includes but is not limited to education records, financial transactions, medical files, criminal records, or employment history.

PII breach.

A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic. This includes, but it not limited to, posting PII on public-facing Web sites (except in the case of approved public affairs releases in accordance with AR 360-1, paragraph 5-3); sending via e-mail to unauthorized recipients; providing hard copies to individuals without a need to know; loss of electronic devices or media storing PII (for example, laptops, thumb drives, compact discs, etc.); use by employees for unofficial business and all other unauthorized access to PII.

Protected identity

A term used in preparation of DA Form 3997, to replace the name and personal data of certain individuals. This term is often used in sensitive cases such as rape or incest.

Provost Marshal/Director of Emergency Services

The senior officer, military or civilian directly responsible for law enforcement and security, regardless of the individual's position or title (for example, security officer, security director, and security manager). This individual must occupy a position that involves the administration of criminal justice.

Serious domestic violence

Any incident of domestic violence where a weapon (such as a firearm, knife or motor vehicle) is involved; the victim suffers a broken limb, is injured during pregnancy, is sexually abused, is choked or strangled or is admitted to the hospital because of injuries incurred during the incident; domestic violence incidents where a violation of a protective order (military or civilian) has occurred.

Serious incident

Any actual or alleged incident, accident, misconduct, or act, primarily criminal in nature, that, because of its nature, gravity, potential for adverse publicity, or potential consequences warrants timely notice to the chain of command.

Serious Incident Report

A formal notification to the chain of command of a serious incident as prescribed by this regulation.

Subject (same as offender)

Person identified and reported by law enforcement officials as the person who committed an offense. Determination that a person committed an offense is based on probable cause supported by corroborating evidence.

Suicide attempt

All overt acts of self-destructive behavior that does not result in death.

Surveillance

Any reported possible activity in which an attempt to record information or to use unusual means to monitor activities is observed. Such attempts will include use of cameras (either still or video), note taking, annotated maps or drawings, hand-drawn maps or diagrams, use of binoculars or other vision-enhancing devices, or any reports from host nation security forces of possible surveillance of U.S. assets.

Suspicious activities/incidents

Any activity/incident that does not specifically fit into one of the other six categories in Chapter 2–5 yet is believed to represent a force protection threat.

Victim

A person who has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime. When a victim is under 18 years of age, incompetent, incapacitated, or deceased, the term includes a spouse, legal guardian, parent, child, sibling, another Family member, or another person designated by the court or the component responsible official or designee

Section III**Special Abbreviations and Terms**

This section contains no entries