

Department of the Army
Headquarters, United States
Training and Doctrine Command
Fort Monroe, Virginia 23651-1047

*TRADOC Regulation 1-8

31 January 2008

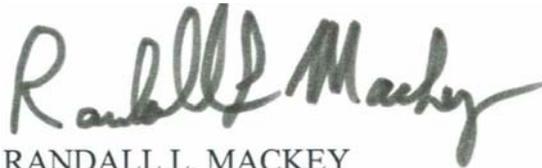
Administration

U.S. ARMY TRAINING AND DOCTRINE COMMAND OPERATIONS REPORTING

FOR THE COMMANDER:

OFFICIAL:

ABRAHAM J. TURNER
Major General, U.S. Army
Acting Deputy Commanding General/
Chief of Staff



RANDALL L. MACKEY
Colonel, GS
Deputy Chief of Staff, G-6

History. This regulation is a rapid action revision. The portions affected by this rapid action revision are listed in the summary of change.

Summary. This regulation prescribes policy and procedures for reporting significant incidents to Headquarters (HQ), United States Army Training and Doctrine Command (TRADOC) using the TRADOC Operations Report and the TRADOC Suspicious Activity Report.

Applicability. This regulation applies to all elements of TRADOC, to include HQ TRADOC, senior commander installations, schools and centers, subordinate commands, activities, and units, including those elements not on an installation with a TRADOC senior commander.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G-3/5/7, Director, Operations, Mobilization, and Readiness Directorate (OMRD). The proponent has the authority to approve exceptions or waivers to this supplement that are consistent with controlling law and regulations. The proponent may delegate this approval authority in writing, to a division chief with the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through higher headquarters to the policy proponent.

* This regulation supersedes TRADOC Regulation 1-8, dated 7 July 2006.

TRADOC Reg 1-8

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 (Management Control).

Supplementation. Supplementation of this supplement is prohibited without prior approval from the Deputy Chief of Staff, G-3/5/7, Director, OMRD (ATTG-ZOO), 5 Fenwick Road, Fort Monroe, VA 23651-1067.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Deputy Chief of Staff, G-3/5/7, Director, OMRD (ATTG-ZOO), 5 Fenwick Road, Fort Monroe, VA 23651-1067. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal).

Distribution. This publication is available only on the TRADOC Homepage at <http://www.tradoc.army.mil/tpubs/supplndx.htm>.

Summary of Change

TRADOC Regulation 1-8

U.S. Army Training and Doctrine Command Operations Reporting

This rapid action revision, dated 31 January 2008-

- o Changes proponent from Deputy Chief of Staff for Operations and Training to Deputy Chief of Staff, G-3/5/7.
- o Adds rationale for submitting Operational Reports and their use by U.S. Army Training and Doctrine Command (para 1-1).
- o Assigns the Deputy Chief of Staff, G-6 the responsibility to update guidance regarding the loss or compromise of personally identifiable information (para 1-4f).
- o Deletes the Threat and Local Observation Notice reporting requirement (para 2-1b).
- o Categorizes incidents into general categories for ease of use (para 2-2).
- o Requires reporting the death of any Soldier (para 2-2b(1)).
- o Requires reporting the deaths of family members and DA civilians on an installation with a U.S. Army Training and Doctrine Command Senior Commander, except for deaths occurring due to natural causes in medical treatment facilities. Requires reporting the death of U.S. Army Training and Doctrine Command family members or U.S. Army Training and Doctrine Command Department of the Army civilians that occur off an installation, only if they are suspected to be criminal in nature (para 2-2b(2)).
- o Clarifies reporting requirement for serious or life threatening injury/illness (paras 2-2b(3) and 2-2b(4)).
- o Adds reporting of communicable/infectious diseases that impact training (paras 2-2b(5) and 2-2b(6)).
- o Refers to DA Pam 600-24 for definition of attempted suicide and requires indicating initial entry training status for suicides/attempted suicides of initial entry training Soldiers (para 2-2b(7)).
- o Adds training use of riot control agents/chemical/biological simulators release outside established parameters as a reportable incident (para 2-2b(8)).
- o Adds any reportable incident or event involving Soldiers (regardless of Army Command) assigned or attached to Warrior Transition Units on an installation with a U.S. Army Training and Doctrine Command Senior Commander (para 2-2b(9)).

TRADOC Reg 1-8

- o Clarifies reportable aircraft accidents/incidents into classes A, B, and C (para 2-2c).
- o Clarifies reporting of sexual assault and domestic abuse incidents (unrestricted reporting and sanitized reporting of restricted reports) (paras 2-2d(4) and 2-2o(3)).
- o Clarifies loss or theft of chemical agents, research chemical agents, biological agents, or radiological material as reportable (para 2-2e(4)).
- o Requires reporting of actual or attempted break-ins of arms rooms or storage areas for arms, ammunition, and explosives; armed robbery or attempted armed robbery of arms, ammunition, and explosives; any evidence of trafficking of arms, ammunition, and explosives; and any incidents involving firearms that cause injury or death (para 2-2g).
- o Updates guidance on reporting requirements for Information Assurance Vulnerability Assessment compliance, computer and network intrusions, compromised computers, and command, control, communications and computers degradations per U.S. Army Training and Doctrine Command Guidance # 06-003 (para 2-2h(1)).
- o Requires reporting of all incidents of lost, stolen or compromised personally identifiable information (para 2-2h(4)).
- o Clarifies reportable chemical/radiological events (para 2-2i).
- o Adds reporting requirement for incidents involving prisoners in Army confinement/correctional facilities on installations with a U.S. Army Training and Doctrine Command Senior Commander (para 2-2r).
- o Adds reporting requirement for electronic eavesdropping/monitoring conversations per AR 190-30, AR 190-53, AR 380-13, and AR 525-1 (para 2-2s).
- o Replaces U.S. Army Training and Doctrine Command Spot Report with U.S. Army Training and Doctrine Command Suspicious Activity Report (paras 2-3 and 3-2, and app C).
- o Changes telephonic notification requirement from 2 hours to immediately upon discovery or notification of an incident at the installation, Headquarters, U.S. Army Cadet Command, or Headquarters, U.S. Army Recruiting Command level (para 3-1a).
- o Includes requirement for copying and pasting Operations Report summary into the e-mail body (para 3-1b).
- o Changes U.S. Army Training and Doctrine Command Guidance Policy #04-001 to U.S. Army Training and Doctrine Command Guidance Policy #06-003 (para 3-1c).
- o Includes requirement to report lost personally identifiable information to the U.S. Computer Emergency Response Team and to the Department of the Army Privacy Office within 1 hour of

discovery and completion of Personally Identifiable Information Incident Report (paras 3-1d(1) and 3-1d(2)).

- o Changes the Suspicious Activity Report incident notification timelines to telephonic notification within 30 minutes and the written Suspicious Activity Report within 4 hours (para 3-2a).
- o Changes the Operations Report format to the Serious Incident Report format in accordance with AR 190-45 (appendix B).
- o Adds U.S. Army Training and Doctrine Personally Identifiable Information Incident Report (appendix D).
- o Adds Management Control Checklist (appendix E).

TRADOC Reg 1-8

Contents

	Page
Chapter 1 Introduction	7
1-1. Purpose	7
1-2. References	7
1-3. Explanation of abbreviations and terms	7
1-4. Responsibilities.....	7
Chapter 2 Reporting Policy.....	8
2-1. Policy	8
2-2. OPREP reportable events and incidents	8
2-3. Suspicious Activity Report (SAR) reportable events and incidents.....	13
Chapter 3 Reporting Procedures	14
3-1. OPREP time requirements and means of reporting.....	14
3-2. SAR time requirements and means of reporting	17
3-3. Handling of reports.....	17
3-4. Required information.....	18
3-5. Parallel report	18
Appendixes	
A. References	19
B. Operations Report Format Example.....	21
C. TRADOC Suspicious Activity Report Format Example	23
D. Personally Identifiable Information Incident Report	25
E. Management Control Checklist.....	26
Glossary	28

Chapter 1 Introduction

1-1. Purpose

To establish policy and procedures for the reporting of significant incidents involving U.S. Army Training and Doctrine Command (TRADOC) senior commander (SC) installations, TRADOC schools and centers, TRADOC subordinate commands, and Department of Defense (DOD) and Headquarters (HQ), Department of the Army (DA) personnel within the TRADOC area of responsibility. The primary purpose of the Operations Report (OPREP) is to provide a means to inform TRADOC senior leadership and HQDA of incidents which impact TRADOC elements. The secondary purpose is to provide HQ TRADOC staff the data to perform trend analysis, develop mitigation policies, and to analyze and integrate the data into the appropriate forums to refine procedures and mitigate incidents.

1-2. References

Required and related publications and prescribed and referenced forms are listed 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

TRADOC SCs, TRADOC school and center commandants, TRADOC subordinate commanders, TRADOC activity, unit, and HQ TRADOC element personnel will ensure that the policies and procedures of this regulation are implemented in their organizations.

a. TRADOC SCs, TRADOC school and center commandants, TRADOC subordinate commanders, TRADOC activity, unit, and HQ TRADOC element personnel are responsible for reporting the events and incidents defined in paragraph 2-2, as well as any other matter that commanders determine to be of concern to the Commanding General (CG), TRADOC.

b. Commander, U.S. Army Accessions Command (USAAC) will ensure subordinate commands report events and incidents defined in paragraph 2-2, as well as any other matter that the commander determines to be of interest to the CG, TRADOC. Commander, USAAC will ensure:

(1) Commander, U.S. Army Cadet Command (USACC) reports incidents in accordance with (IAW) this regulation involving cadre or students at Senior Reserve Officers' Training Corps units/activities.

(2) Commander, U.S. Army Recruiting Command (USAREC) reports incidents IAW this regulation involving recruiters, recruits at Army recruiting stations, incidents involving Army recruiting stations, and the Hometown Recruiter Program.

c. Deputy Chief of Staff (DCS), G-3/5/7, Director, Operations, Mobilization, and Readiness Directorate (OMRD) or an OMRD representative is responsible for notifying the TRADOC Command Group and TRADOC Staff of significant OPREPs.

TRADOC Reg 1-8

d. DCS, G-3/5/7, Director, Command Provost Marshal Directorate (CPMD) or a CPMD designated representative will analyze each Suspicious Activity Report (SAR) and forward reports to the TRADOC Deputy Chief of Staff, G-2.

e. TRADOC Emergency Operations Center (EOC) is responsible for collecting, analyzing, and referring all OPREPs, SARs, and Serious Incident Reports (SIR) to the Director, OMRD, TRADOC leadership, and to appropriate HQ and staff sections. The TRADOC EOC will receive OPREPs, request follow-up reports and report incidents to the TRADOC leadership.

f. DCS, G-6 is responsible for updating personally identifiable information (PII) guidance, as necessary.

Chapter 2 Reporting Policy

2-1. Policy

a. Report incidents to HQ, TRADOC, as defined in paragraph 2-2. The list is not inclusive. Commanders should report any incident that might concern the CG, TRADOC as a serious incident, regardless of whether specifically listed. In determining whether an event/incident is of concern to CG, TRADOC, the following factors should be considered: the severity, the potential for publicity, and the potential consequences of the event/incident. In case of doubt, submit an OPREP.

b. Reporting procedures outlined in this regulation do not replace the reporting procedures as outlined in AR 190-45 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 in accordance with (IAW paragraph 5-3 of this regulation.

2-2. OPREP reportable events and incidents

Use the OPREP for all significant incidents occurring on a TRADOC SC installation and in its geographical area of responsibility as outlined in AR 190-45, table 1-1. When a Soldier is listed as a subject in an OPREP include whether the Soldier has deployed within the past year. At a minimum, commanders must report:

a. All category 1 SIR reportable incidents in AR 190-45, paragraphs 8-2a through 8-2h, involving TRADOC personnel and assets are reportable.

b. The following category 2 SIR incidents and TRADOC specific incidents to include accidents, incidents, or medical situations resulting in:

- (1) Any death of a service member that occurs on or off an installation.

(2) The death of a family member or DA civilian that occurs on a TRADOC SC installation, except for deaths occurring due to natural causes in medical treatment facilities. The death of a TRADOC family member or TRADOC DA civilian that occurs off an installation is reportable only when the death is suspected to be criminal in nature. When the cause of death is unknown, report it as “undetermined manner of death.” The report should also include when the next of kin were notified, and in the case of vehicle accidents, whether or not seatbelts were used, and if alcohol was involved.

(3) Serious injury or illness of a TRADOC Soldier that creates a danger of loss of life, limb, or eyesight.

(4) Life threatening injury or illness of a TRADOC family member.

(5) Significant environmental injury to TRADOC Soldiers and family members, that could impact or potentially impact TRADOC missions (such as heat stroke, rhabdomyolysis, carbon monoxide poisoning, hypothermia, frostbite, heat exhaustion, and communicable illnesses, such as influenza, hepatitis, and West Nile virus). Consult with the local medical treatment facility to determine the significance of these events; see AR 40-5, paragraph 2-18d, for DOD reportable medical events.

(6) Communicable illnesses that exceed the expected baseline for those illnesses and unusual illnesses, such as avian influenza. Consult with the local medical treatment facility.

(7) Suicide (all overt acts of self-destructive behavior that result in death) or attempted suicide (all overt acts of self-destructive behavior that does not result in death) by a Soldier, family member or DA civilian occurring on a TRADOC SC installation, and suicide or attempted suicide by a Soldier occurring off an installation. If suicide or attempted suicide involves a Soldier attending initial entry training (basic combat training, advanced individual training, and one station unit training) then indicate initial entry training status in the OPREP summary of incident section. (See DA Pam 600-24 for suicide prevention information).

(8) Training use of riot control agent or chemical biological simulator release outside of established parameters.

(9) Any reportable incident or event involving Soldiers (regardless of Army Command (ACOM)) assigned or attached to warrior transition units on installations with a TRADOC SC.

c. Aircraft accident or incident (Class A, B, and C only).

(1) Manned aircraft accidents or incidents. Any type of aircraft accident or incident that causes damage to aircraft or injury to personnel. Reporting requirements extend to tenant or transient aircraft from another Service or ACOM using TRADOC facilities or land in the geographic area of responsibility.

(2) Unmanned aircraft accident or incidents. Any type of unmanned aerial vehicle accident or incident that causes damage to the vehicle or injury to personnel. Reporting requirements

TRADOC Reg 1-8

extend to tenant or transient aircraft from another service or ACOM using TRADOC facilities or land in the geographic area of responsibility.

d. Criminal activity.

(1) Serious crimes (for example, aggravated assault, sexual assault, kidnapping, larceny exceeding \$50,000, and murder or attempted murder committed by or against a Soldier, family member, or DA civilian).

(2) Major fires, arson, and natural disasters resulting in death, serious injury, or property damage exceeding \$50,000.

(3) Racially or ethnically motivated criminal acts.

(4) When sexual assault victims elect the restricted reporting option, report only the following sections: the reporting individual's name (operations center watch officer, unit representative, etc.), date of initial report, installation name, and summary of incident. Write "Restricted report/Sexual assault" in the summary of incident section. All the other OPREP sections are to remain blank.

e. Property theft/loss.

(1) Property damage or loss of property or equipment exceeding \$50,000.

(2) Theft, suspected theft, loss, wrongful appropriation, or willful destruction of government property (appropriated or non-appropriated funds) valued at more than \$50,000.

(3) Theft, suspected theft, loss or recovery of sensitive items, and the discovery of a loss of accountability (for example, night vision devices, classified material (excluding For Official Use Only (FOUO)) and controlled cryptographic items).

(4) Loss or theft of any chemical agent, research chemical agent, biological agent, or radioactive material.

f. Wrongful possession, manufacturing, and distribution of narcotics, stimulants, depressants, hallucinogens, anabolic steroids, and chemicals used in the illicit production of controlled substances. See AR 190-45, paragraph 8-3e, for the minimum reportable amounts.

g. Arms, ammunition, and explosives (AA&E). Theft, suspected theft, loss, or recovery of weapons, explosives, and munitions in the types and quantities listed below:

(1) Any missile, rocket, mine, artillery, or mortar rounds.

(2) Any machine gun or automatic weapon.

(3) Any fragmentation, concussion, high explosive grenade, or other type of simulator or device containing explosive materials, including artillery or ground burst simulators.

(4) Any explosives, to include demolition explosives.

(5) Any type of small arms ammunition (5.56mm, 7.62mm, or 9mm) in the amount of 200 rounds or greater.

(6) Any amount of ammunition of any type greater than .50 caliber.

(7) Any type of .50 caliber ammunition in the amount of 100 rounds or greater.

(8) Any type of blank ammunition when the amount is equal to or greater than the issue amount in a wire bound wooden box.

(9) Additionally, report actual or attempted AA&E break-ins of arms rooms or storage areas; AA&E armed robbery or attempted armed robbery; any evidence of AA&E trafficking; and any incidents involving firearms that cause injury or death.

h. Command, control, communications, and computers (C4) outages/information systems intrusions/PII.

(1) All significant, unplanned degradations of C4 assets (as defined in TRADOC Command Guidance #06-003) occurring at a TRADOC activity or in the installation operations center (IOC). Significant degradation is defined as the loss of 50 percent or greater of a specific communications capability inhibiting the ability of the SC to exercise command and control longer than two hours.

(2) Major installation power outages that impact operations and training.

(3) Information system intrusions (both suspected and confirmed), to include incidents of hacking of government web sites.

(4) Report all incidents of lost, stolen, or compromised PII in electronic or physical form. Current TRADOC guidance memorandum, subject: Reporting the Loss of Personally Identifiable Information provides detailed reporting procedures and is located on the Army Knowledge Online, TRADOC Deputy Chief of Staff, G-6 page titled "Command Guidance" at <https://www.us.army.mil/suite/page/309>.

i. Trainee abuse and drill sergeant misconduct.

(1) Allegations of trainee abuse as defined in TRADOC Reg 350-6, paragraph 2-5 (any improper or unlawful physical, verbal, or sexual act against a trainee; does not include acts involving a trainee against trainee). However, if the credibility of the allegation can be quickly assessed (within two hours) and the command considers it not credible, an OPREP is not required. The non-credible allegation will be recorded and kept on file at the unit.

TRADOC Reg 1-8

(2) Allegations of drill sergeant misconduct not related to trainee abuse.

j. Bomb threats at TRADOC SC installations, TRADOC schools and centers, and TRADOC activities and units on other installations, to include Reserve Officers' Training Corps brigades, battalions, companies, detachments, and recruiting stations.

k. Environmental accidents or incidents at an installation with a TRADOC SC that result in:

(1) Any release of a hazardous substance (to include fuel) resulting in injury, death, 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).

(2) 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.)

l. Chemical or radiological event.

(1) A chemical or radiological event encompassing chemical surety or 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 chemical surety or radiological material, or any event of concern to the local commander or director of the chemical surety or radiological training facility that potentially impacts the mission.

(2) Any potential chemical agent exposure resulting in greater than 10 percent depression of red blood cell cholinesterase through initial lab analysis.

m. Change in threat or force protection condition.

n. Incidents/accidents involving international students and personnel assigned to TRADOC commands, schools, centers, or activities. Reportable incidents/accidents include absent without leave, disciplinary problems, any training accident, or any accident causing injury or death.

o. Child abuse and domestic violence.

(1) Actual or alleged child abuse that takes place within an Army organizational setting or facility (that is, a child development center, youth activities center, medical treatment facility,

gymnasium, etc.) or an Army sponsored or sanctioned activity (that is, quarters based family child care home, youth sports, or recreation activities, field trips, etc.).

(2) Incidents of actual or alleged child abuse occurring within the family unit which involve the use of a weapon (such as a firearm, knife, or other devices, which may cause serious bodily injury) or where the victim suffers a broken limb, is sexually abused, choked, strangled, or is admitted to the hospital due to injuries incurred during the incident.

(3) Any incident of domestic violence incidents (violence against a family member or person residing in the home or quarters of a military sponsor or as otherwise defined by state law that involves the use of a weapon, such as a firearm, knife or similar instruments that may cause serious bodily injury or that results in the victim being admitted to the hospital because of the injuries received, or when the victim is sexually abused, choked, or strangled). In cases of restricted reporting of domestic violence, only complete the following sections: reporting individual's name (operations center watch officer, unit representative, etc.), date of initial report, installation name, and summary of incident. Write "Restricted report/Domestic violence" in the summary of incident section. All the other OPREP sections are to remain blank.

p. Significant violations of Army Standards of conduct, to include bribery, conflict of interest, graft, or acceptance of gratuities.

q. Any incident, event, or accident that may generate adverse publicity.

r. Incidents involving prisoners or detainees of Army confinement or correctional facilities on an installation with a TRADOC SC, to include escape from confinement or custody, disturbances which require the use of force, wounding, or serious injury to a prisoner, and all deaths.

s. Violations of Army policy as it pertains to monitoring and recording of conversations (see AR 190-30, AR 190-53, AR 525-1) or acquisition and storage of non-affiliated U.S. person information (see AR 380-13).

2-3. Suspicious Activity Report (SAR) reportable events and incidents

The intent of suspicious activity reporting is to ensure the TRADOC leadership has a clear picture of the scale of these phenomena by capturing the information. The raw data information collected and reported on the SAR allows the intelligence community to analyze trends and provide actionable intelligence for commanders to use in decision making. Reportable suspicious incidents include, but are not limited to the following criteria:

a. Non-specific threat. A non-specific threat received by any means, which states 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).

b. Surveillance. Any reported possible surveillance in which an attempt to record information or to use unusual means to monitor U.S. assets or activities is observed. Such attempts may

TRADOC Reg 1-8

include use of cameras (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.

c. 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.

d. 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.

e. 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.

f. 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; and thefts of military uniforms which may be used to gain access to a military installation, vandalism, etc.

Chapter 3 Reporting Procedures

3-1. OPREP time requirements and means of reporting

a. Incidents will be reported to the TRADOC EOC immediately upon discovery or notification at the installation, HQ, USAREC, or HQ, USACC level. The reporting command will notify the TRADOC EOC by the fastest means possible, either telephonic or e-mail. Call Defense Switched Network (DSN) 680-2256, commercial (757) 788-2256, or e-mail to tradoc.eocwatch@conus.army.mil. The EOC is operational 24 hours a day. Timeliness takes precedence over completeness for the initial report. Notification to the TRADOC EOC by the reporting agency (IOC, Command Operations Center, etc.) must be done immediately utilizing the methods stated above. See figure 3-1 for the TRADOC OPREP notification process.

b. Reporting installations will prepare and forward an initial OPREP message, using format at appendix B, by e-mail to tradoc.eocwatch@conus.army.mil or facsimile (757) 788-2997 or DSN 680-2997. Write all the available information in the OPREP summary block. Copy and paste the OPREP summary block into the e-mail body, omitting all PII from the summary. ***Forward initial OPREP message to the TRADOC EOC within four hours of initial***

notification of the incident. OPREP numbering will be in concert with SIR conventions in AR 190-45, figure 9-1.

c. Use TRADOC Command Policy #06-003 report format to report incidents listed in paragraph 2-2h(1).

d. Use the PII Incident Report to report incidents listed in paragraph 2-2h(4). The PII Incident Report is available on the TRADOC homepage at <http://www.tradoc.army.mil/tpubs/TRADOCforms.htm>. A PII Incident Report example is provided in appendix D. Commanders will ensure the additional PII incident notification requirements, listed below, are followed and delegate execution to a level that supports compliance.

(1) Report to the Department of Homeland Security, U.S. Computer Emergency Response Team (US-CERT) within 1 hour of discovery. Use the US-CERT web-based reporting system at <https://forms.us-cert.gov/report/>. US-CERT will e-mail the individual submitting the report a receipt confirmation and report number. Write this US-CERT report number on the TRADOC PII Incident Report.

(2) At the same time the US-CERT is notified, submit an e-mail notification to the DA Freedom of Information Privacy Act Office at PII.REPORTING@US.ARMY.MIL. This e-mail will include the following information: organization involved, date of incident and number of personnel potentially impacted, brief synopsis, and point of contact information.

(3) The agency notifications in subparagraphs (1) and (2), above, are sent directly to those agencies. TRADOC leadership does not see these notifications.

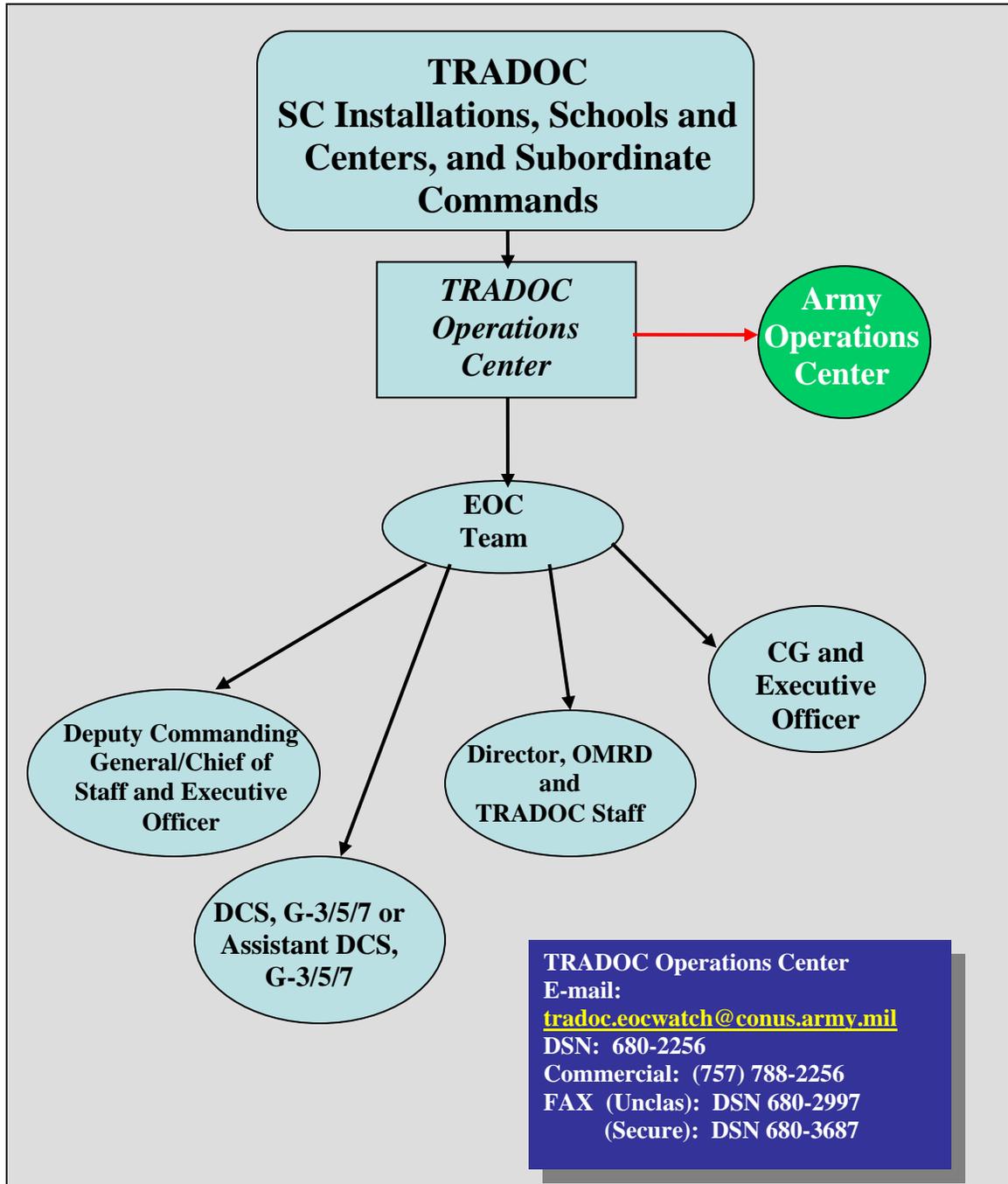


Figure 3-1. TRADOC OPREP Notification Process

3-2. SAR time requirements and means of reporting

a. Submit written SARs to the TRADOC EOC within 4 hours of the incident in the SAR format. Telephonically notify the TRADOC EOC within 30 minutes of discovery or notification of the suspicious activity. Classification of the initial SAR is unclassified. The reporting command will provide initial notification to the TRADOC EOC IAW paragraph 3-1a above.

b. Installations will provide a complete SAR within 4 hours of the incident. When written or electronic reports are used installations must call the TRADOC EOC to confirm receipt.

c. When reporting an incident the “summary of incident” block of the SAR will answer the who, what, when, where, why and how, in addition to the following:

- (1) Initial response or action taken.
- (2) Indication of whether the incident is open or closed and resolved or unresolved.
- (3) Source and assessment of credibility of the source.
- (4) Coordinating agencies (for example, Federal Bureau of Investigation).

d. A follow-up report will be submitted after the final determination has been made for each incident.

(1) For incidents determined to be unfounded, provide a telephonic report, followed by a supplemental SAR to the EOC.

(2) For incidents determined to be founded, provide telephonic report, followed by a supplemental SAR with pertinent attachments (for example, the SIR), if applicable.

e. The TRADOC SAR format is located at appendix C.

3-3. Handling of reports

a. Due to the potential sensitive nature of OPREPs, all OPREP e-mails and reports will be marked FOUO. Data sent as FOUO will be digitally signed and encrypted using common access card/Public Key Infrastructure. In addition, installations will use their Role Based certificate account to help reduce proliferation.

b. Health Insurance Portability and Accountability Act (HIPAA) considerations. IOCs will only transmit personal information in OPREPs as it relates to the OPREP incident. IOCs will not report unrelated patient health information in an OPREP to a third party without the patient's consent IAW the HIPAA.

TRADOC Reg 1-8

3-4. Required information

a. The OPREP report format is located appendix B. Reports will include all available, relevant facts. OPREPs provided telephonically and via e-mail will identify individuals by rank, name, unit of assignment, and ACOM. If the reporting command believes that the protection of the individual's identity is necessary, do not submit name(s), age, race, position, or unit.

b. When reporting training deaths, complete line 8a through 8j of the OPREP (see app B).

3-5. Parallel report

All HQ TRADOC elements receiving parallel or courtesy reports will verify that the EOC is aware of the incident. Command and staff agencies will notify the TRADOC EOC of any reports to permit tracking of information on the incident.

Appendix A References

Section I

Required Publications

ARs, DA pams, and DA forms are available at [Army Publishing Directorate \(APD\) - Home Page](#). TRADOC publications and forms are available at [TRADOC Publications](#).

AR 190-30

Military Police Investigations

AR 190-45

Law Enforcement Reporting

AR 190-53

Interception of Wire and Oral Communications for Law Enforcement Purposes

AR 200-1

Environmental Protection and Enhancement

AR 380-13

Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

AR 525-1

DA Command and Control System (DACCS)

DA Pam 600-24

Suicide Prevention and Psychological Autopsy

TRADOC Reg 350-6

Enlisted Initial Entry Training (IET) Policies and Administration

TRADOC Command Guidance #06-003

Information Assurance Vulnerability Alert (IAVA) Compliance, Computer and Network Intrusion, Compromised Computer, and Command, Control, Communications, and Computer (C4) Degradations Reporting

TRADOC Memorandum

Subject: Reporting the Loss of Personally Identifiable Information

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.

TRADOC Reg 1-8

AR 11-2
Management Control

AR 40-5
Preventive Medicine

Section III Prescribed Forms

This section contains no entries.

Section IV Referenced Forms

This section contains no entries.

Appendix B
Operations Report Format Example

From: CDRUSAICS Ft Benning GA//OFC SYMBOL//
TO: CDRUSATRADOC Ft Monroe VA//ATTG-ZOO
tradoc.eocwatch@conus.army.mil
Info: IMCOM Opns Ctr

Subj: OPREP Number 07-0000 (Initial/Update/Final)

1. Category: 2
2. Type of incident: Heat Stroke/Death
3. Date/time of incident/DTG Received in IOC: 010730 July 07/011000 July 07
4. Location: Sand Hill, IBCT HQ
5. Other information:
 - a. Racial: no
 - b. Trainee involvement: yes
6. Personnel involved:
 - a. Subject
 - (1) Name: Doe, John
 - (a) Pay grade: PV2
 - (b) SSN: 123-45-6789
 - (c) Race: White
 - (d) Sex: Male
 - (e) Age: 18
 - (f) Position: Trainee
 - (g) Security Clearance: S-NAC
 - (h) Unit and station: A Co, 2-29 IN (TRADOC)
 - (i) Duty Status: Present
 - b. Victim: N/A
7. Summary of incident: At approximately 010730 Jul 07, while conducting PT PV2 Doe complained of headache, nausea, and muscle cramps. Immediately SSG Smith took his core body temp at 105.3 and applied ice sheets and started an IV. Emergency Medical Services (EMS) personnel were called and PV2 Doe was transported to MACH. His body temp was 105.1 upon arrival at MACH. At approximately 010845 Jul, PV2 Doe went into massive renal failure and died.
8. Remarks:
 - a. Next of Kin Notification: Yes, parents

TRADOC Reg 1-8

- b. Soldier Deployed w/i last year: No
 - c. Were seatbelts worn: N/A
 - d. Was alcohol involved: N/A
 - e. Was personal protective gear/equipment worn: N/A
 - f. Any previous medical history: UNK
 - g. Were Combat Lifesavers present: Yes
 - h. Was CPR performed at the scene: No
 - i. Anyone notice anything different concerning Soldier's performance: Yes. Unstable, ungainly gait.
 - j. Times leading up to Soldiers Death:
 - (1) Time CPR started: N/A
 - (2) Time 911 called: 0735
 - (3) Time EMS personnel arrived on scene: 0745
 - (4) Time EMS departed scene en route to hospital: 0750
 - (5) Time EMS arrived at hospital: 0800
 - (6) Time Soldier pronounced dead: 0845
 - k. Soldier's Component: AD
 - l. Ages/gender of family members: N/A
 - m. Type of Training: One station unit training
 - n. Phase of Training: 3d week
 - o. Weather conditions at time of incident: Overcast, temp in low 70's
 - p. Other factors contributing to the incident:
9. Publicity: None expected at this time
10. Commander Reporting: COL I.M. Short, COS
11. Point of Contact: SFC Dill, SDNCO, DSN 835-0000, BENN.DOT.EOC@benning.army.mil
12. Downgrading instructions: The FOUO protective marking may be removed on DDMMYYYY.

Appendix C
TRADOC Suspicious Activity Report Format Example

TRADOC SUSPICIOUS ACITIVITY 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: (Non-specific threat/ Surveillance/ Elicitation/ Tests of security/ Intrusions/ Repetitive activities/ Suspicious activities/Incidents)

a. Non-specific threat. A non-specific threat received by any means, which contain 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).

b. 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, 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.

c. 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.

d. 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.

e. 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.

f. 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

TRADOC Reg 1-8

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 Camp Gate, Ft Patton, VA.)

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 Camp 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, Garrison Commander, COL XXXX on DD MMM YY)

11. ACTION(S): (For example, incident was reported to local police, Criminal Investigation Division (CID) or Military Intelligence (MI) and they have taken the lead in the investigation; or the above information was passed on to _____ and they have taken the lead for investigative action.)

12. FOLLOW-UP:

13. PERSON(S)/AGENCIES INVOLVED: (For example, witness, antiterrorism officer, MI, CID, provost marshal office, local law enforcement, etc.)

14. REPORT RECEIVED BY: (Name and position of individual initiating the report.)

Appendix D
Personally Identifiable Information Incident Report

TRADOC	
PERSONALLY IDENTIFIABLE INFORMATION (PII) INCIDENT REPORT	
(blocks marked with * indicate required items for United States Computer Emergency Readiness Team (US-CERT) on-line Report)	
IMPACT CATEGORY	
<input type="checkbox"/> High Impact (> or = 500 individual PII on the system) <input checked="" type="checkbox"/> Medium Impact (< 500 individual PII on the system) <input type="checkbox"/> Unknown Impact	Actual number of PII <input style="width: 50px;" type="text"/> OR Estimated number of PII <input style="width: 50px; text-align: center; value: 99;" type="text"/>
REPORTING ORGANIZATION	
1. ORGANIZATION xxxx Recruiting Station, Lansing, MI - USAREC	2. POINT OF CONTACT NAME/ TELEPHONE/ EMAIL: CPT John Smith/ 517-111-1111/ cptjohn.smith@us.army.mil
3. DATE/ TIME REPORTED TO US-CERT (include tracking number): 5 Sep 07/ 1400 (USCERT06822)	4. * INDIVIDUAL REPORTING TO US-CERT (Name/Email/ Contact Number): SFC John Smith/ 517-111-1111/ stcjohn.smith@us.army.mil
INCIDENT INFORMATION	
5. TYPE OF REPORT: <input checked="" type="checkbox"/> Initial <input type="checkbox"/> Follow-up <input type="checkbox"/> Final	6. *DATE/TIME INCIDENT OCCURRED (local time) * Time Zone 5 Sep 07/ 1200-1300 CST
7. WAS THE DATA ENCRYPTED? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO If data was encrypted, what Data-at-Rest solution was implemented? POINTSEC	
8. * LAW ENFORCEMENT NOTIFICATIONS MADE (Civilian and Military)(Agency names and case numbers): Lansing Police Department - case number LPD 174-2007	
9. PROVIDE SHORT DESCRIPTION OF THE INCIDENT AND POTENTIAL IMPACT THE LOSS OF PII WILL HAVE ON THE COMMAND: Brief description of incident, type of information lost and notifications either made or will make to individual(s) whose information was compromised: Active duty recruiter secured an assigned government laptop with a cable lock to an immobile object in the recruiting station and went to lunch at a local nearby establishment. Upon return, it was discovered that the recruiting station front door window was smashed and the cable lock had been cut by person(s) unknown with an unknown device. The laptop contained personally identifiable information for approximately 99 civilian potential recruits consisting of name, social security number, home address, and home telephone number. Replication of the last hard drive image will be conducted in order to obtain a better determination of affected individuals so they can be notified of the incident and provided additional information to assist the affected members in understanding the potential risks and precautions they can take to protect their identities. Local police were immediately notified. United States Computer Emergency Readiness Team (US-CERT) was notified at the lowest level possible in order to meet the one-hour reporting requirement via their web based reporting system. Immediately after notifying US-CERT, an email was sent to pii.reporting@us.army.mil providing a brief synopsis and point of contact information. The potential impact is minimized as the laptop and the data contained on the laptop was encrypted with an Army-approved data at rest solution. Investigation continues by local police.	
10. * OPERATING SYSTEM (OS) OF AFFECTED COMPUTER(S):	XP
11. * ADDITIONAL OS AND PATCH INFORMATION (if not know enter "Unknown"):	Unknown
12. * LOCATION OF SYSTEM AFFECTED (City/State):	Lansing, MI
13. * INCIDENT CATEGORY TYPE:	
<input type="checkbox"/> CAT 0 - Exercise/ Network Defense Testing <input type="checkbox"/> CAT 1 - Unauthorized Access <input type="checkbox"/> CAT 2 - Denial of Service <input type="checkbox"/> CAT 3 - Malicious Code <input type="checkbox"/> CAT 4 - Improper Usage <input type="checkbox"/> CAT 5 - Attempted Access <input checked="" type="checkbox"/> CAT 6 - Under Investigation	
14. OTHER NOTIFICATIONS COMPLETED. (list date/time, organization and title of Individual) (i.e. 1530hrs, 4 Nov 06, USAAC Commander and PAO): USAAC Command Operations Center was notified at 0900hrs, 5 Sep 07; USAAC Command was notified at 0930hrs; USAAC Public Affairs Officer was notified at 1000hrs	
15. ACTIONS TAKEN BY THE COMMAND/ REMARKS (i.e. PIA conducted, letters of notification completed on 4 Nov 06, PAO issued statements, etc): Letters of notification will be sent out NLT than 10 days.	

TRADOC PII INCIDENT REPORT (FEB 2007)

Figure D-1. Personally Identifiable Information Incident Report Example

TRADOC Reg 1-8

Appendix E Management Control Checklist

E-1. Function

The function covered by this checklist is the administration of operations reporting within TRADOC.

E-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.

E-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 five years.

E-4. Test questions

- a. Is the correct format used for OPREPs (SIR format in AR 190-45)?
- b. Are initial telephonic/e-mail notifications of OPREP incidents reported to the TRADOC EOC immediately upon discovery or notification at the installation, HQ, USACC, or HQ, USAREC level?
- c. Are initial written OPREPs sent to TRADOC EOC within 4 hours of initial discovery or notification at the installation, HQ, USACC, or HQ, USAREC level?
- d. Do initial OPREPs contain all the relevant information (who, what, when, where, how and why) available at the time?
- e. Are follow-ups forwarded to the TRADOC EOC within 2 hours of the request for follow-up information?
- f. Are OPREPs digitally signed and encrypted from the originator through all the intermediate approval levels to the TRADOC EOC?
- g. Are SARs used IAW paragraph 2-3 of this regulation?
- h. Are SARs submitted to the TRADOC EOC within 30 minutes of knowledge of the incident?
- i. Does the TRADOC staff conduct trend analysis and provide feedback on identified trends to the TRADOC leadership and SCs on a routine basis?

E-5. Suppression

No previous management control evaluation checklist exists for this program.

E-6. Comments

Help to make this a better tool for evaluating management controls. Submit comments directly to Director, OMRD, DCS, G-3/5/7 (ATTG-ZOO), 5 Fenwick Road, Fort Monroe, VA 23651.

TRADOC Reg 1-8

Glossary

Section I

Abbreviations

AA&E	arms, ammunition, and explosives
ACOM	Army command
C4	command, control, communications, and computers
CG	commanding general
CID	Criminal Investigation Division
CPMD	Command Provost Marshall Directorate
CPR	cardiopulmonary resuscitation
DA	Department of the Army
DCS	deputy chief of staff
DOD	Department of Defense
DSN	Defense Switched Network
EMS	Emergency Medical Services
EOC	Emergency Operations Center
FOUO	For Official Use Only
G-2	intelligence
G-3/5/7	operations, plans, and training
G-6	command, control, communications, and computers
HIPAA	Health Insurance Portability and Accountability Act
HQ	headquarters
HQDA	Headquarters, Department of the Army
IAW	in accordance with
IOC	installation operations center
MI	military intelligence
OPREP	operations report
OMRD	Operations, Mobilization, and Readiness Directorate
PII	personally identifiable information
SIR	serious incident report
SC	senior commander
SAR	Suspicious Activity Report
TRADOC	U.S. Army Training and Doctrine Command
USAAC	United States Army Accessions Command
USACC	United States Army Cadet Command
USAREC	United States Army Recruiting Command
US-CERT	United States Computer Emergency Readiness Team

Section II
Terms

Family member

Includes those individuals for whom the Soldier 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.

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.

Suicide attempt

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

Section III
Special Abbreviations and Terms

This section contains no entries.