

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

*TRADOC Regulation 1-8

16 November 2010

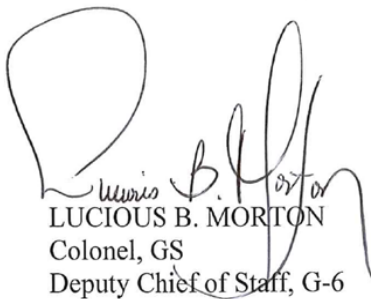
Administration

U.S. ARMY TRAINING AND DOCTRINE COMMAND OPERATIONS REPORTING

FOR THE COMMANDER:

OFFICIAL:

JOHN E. STERLING, JR.
Lieutenant General, U.S. Army
Deputy Commanding General/
Chief of Staff



LUCIOUS B. MORTON
Colonel, GS
Deputy Chief of Staff, G-6

History. This publication 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, Current Operations (G-33). 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

*This regulation supersedes TRADOC Regulation 1-8, dated 31 January 2008.

TRADOC Reg 1-8

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.

Army management control process. This regulation contains management control provisions and identifies key management controls that must be evaluated in accordance with Army Regulation (AR) 11-2 (Manager's Internal Control Program).

Supplementation. Supplementation of this regulation is prohibited without prior approval from the Deputy Chief of Staff, G-3/5/7, Director, G-33 (ATTG-OPA), 5 Fenwick Road, Fort Monroe, VA 23651-1067.

Suggested improvements. Users are invited to send comments and suggested improvements on Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Deputy Chief of Staff, G-3/5/7, Director, G-33 (ATTG-OPA), 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 16 November 2010-

- o Changes the Army Accession Command's reporting requirements (para 1-4b).
- o Updates reportable events and incidents (para 2-2a).
- o Updates reporting of deaths (para 2-2a(21)).
- o Updates significant command, control, communications, and computers degradation/outage and information systems incident reporting (paras 2-2a(40), 3-1c, and 3-1d).
- o Updates personally identifiable information breach reporting (paras 2-2a(43) and 3-1e).
- o Adds requirement to notify Army Watch within 2 hours of the initial notification to U.S. Army Training and Doctrine Command of "immediate response" request(s) from civil authorities (paras 2-2a(52) and 3-1f).
- o Adds reference to the location of commander's critical information requirement in the U.S. Army Training and Doctrine Command Campaign Plan (para 2-2a(53)).
- o Updates suspicious activity report reporting (para 2-3).
- o Updates reporting procedures (para 3-1b).
- o Adds personally identifiable information breach and notification procedures (app D).
- o Adds command, control, communications, and computer degradation reporting procedures (app F).
- o Updates organization, position titles, and references throughout the publication.

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).

TRADOC Reg 1-8

- 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)).
- 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 2-2l).
- 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, and AR 380-13 (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 3-1e(1) and 3-1e(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	8
1-1. Purpose	8
1-2. References	8
1-3. Explanation of abbreviations and terms	8
1-4. Responsibilities.....	8
Chapter 2 Reporting Policy.....	9
2-1. Policy	9
2-2. Operations report reportable events and incidents	9
2-3. Suspicious activity report (SAR) reporting	17
Chapter 3 Reporting Procedures	19
3-1. OPREP time requirements and means of reporting.....	19
3-2. SAR time requirements and means of reporting	22
3-3. Handling of reports.....	23
3-4. Required information.....	23
3-5. Parallel report	23
Appendix A References	24
Appendix B OPREP Report Form	26
B-1. OPREP report.....	26
B-2. OPREP report format example	26
Appendix C TRADOC SAR Format	28
C-1. TRADOC suspicious activity report.....	28
C-2. TRADOC suspicious activity report format example.....	28
Appendix D PII Breach Reporting Template, Notification, Remedial Actions, and Risk Analysis	30
D-1. DOD PII Breach Reporting Template	30
D-2. Report updates	30
D-3. Notification procedures	30
D-4. Remedial actions.....	32
D-5. Identity theft risk analysis.....	32
Appendix E Management Control Checklist.....	35
E-1. Function.....	35
E-2. Purpose	35
E-3. Instructions.....	35
E-4. Test questions.....	35
E-5. Suppression	35
E-6. Comments	36
Appendix F C4 Degradation Reporting	37
F-1. C4 degradation	37
F-2. Unplanned C4 degradation within IOCs and/or TRADOC activities	37
F-3. Planned C4 degradations within IOCs and/or TRADOC activities	38
Glossary	40

Table List

Table D-1 PII risk assessment model..... 31

Figure List

Figure 3-1. TRADOC OPREP Notification Process 20
Figure 3-2. Example of Suspected or Observed Information System Incident Report 21
Figure B-1. Operations report format example..... 26
Figure C-1. SAR report format example..... 28
Figure F-1. Unplanned C4 outage report 38

TRADOC Reg 1-8

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 below in addition to any other matter that the commander determines to be of interest to the CG, TRADOC. Commander, USAAC will report:

(1) Any incident involving a Ft. Knox Soldier that could possibly create a negative perception for the Army and/or result in adverse media attention.

(2) Any incident that results in death or serious injury to a Soldier or DA civilian.

(3) Allegations of trainee abuse at Ft. Knox.

(4) Any TRADOC resourcing decision that negatively impacts the ability of Ft. Knox to execute its mission, both as Human Resources Command (HRC) Center of Excellence (CoE) and Senior Commander functions.

c. Deputy Chief of Staff (DCS), G-3/5/7, Director, Current Operations (G-33), or a Current Operations (G-33) representative is responsible for notifying the TRADOC Command Group and TRADOC staff of significant OPREPs.

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 Operations Center (TOC) is responsible for collecting, analyzing, and referring all OPREPs, SARs, and serious incident reports (SIR) to the Director, Current Operations (G-33), TRADOC leadership, and to appropriate HQ and staff sections. The TOC 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](#) and [2-3](#). The lists are 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: severity of the incident, potential for adverse publicity, potential consequences of the incident, whether or not the incident is reportable under other reporting systems, effect of the incident on readiness or the perception of readiness. 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](#) (Law Enforcement Reporting) 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 their servicing Army installation provost marshal office (PMO)/Director of Emergency Services (DES) and/or U.S. Army Criminal Investigation Command (USACIDC) office for appropriate inquiry and investigation.

2-2. Operations report reportable events and incidents

Use the OPREP for all significant incidents occurring on- or off-installation that have a TRADOC nexus. TRADOC OPREP reportable incident are similar to, but do not replace Army SIR reportable incidents required by [AR 190-45](#). TRADOC OPREP and Army SIR reportable incidents are parallel reports and both will be submitted, TRADOC OPREPs to TOC and Army SIRs to servicing installation PMO/DES. When a Soldier is listed as a subject in an OPREP, include whether the Soldier has deployed within the past year.

TRADOC Reg 1-8

a. At a minimum, commanders must report actual or alleged incidents involving the following:

(1) On- and off-post riots, serious disturbances, or demonstrations targeted against the Army or involving Army personnel.

(2) War crimes, including mistreatment of enemy prisoners of war, detainees, displaced persons, retained persons, or civilian internees; violations of the Geneva Conventions; and atrocities.

(3) Requests by members of the Army for political asylum in foreign countries or indications of defection.

(4) Terrorist activities, sabotage, and incidents, initiated or sponsored by known terrorists, dissident groups, or criminal elements that occur on an installation or involve military personnel or property off an installation.

(5) Bomb or explosive incidents resulting in death, injury of military personnel, or damage to military property.

(6) Incidents involving material damage that seriously degrade unit operational or training readiness.

(7) Threats against Government weapons and ammunition.

(8) Information on threats, plans, or attempts to harm or kidnap, or other information bearing on the personal security of the President of the United States, Vice President of the United States, or other persons under U.S. Secret Service protection.

(9) Information on threats, plans, or attempts to harm or kidnap, or other information bearing on the personal security of any Army senior leader.

(10) Training use of riot control agent or chemical/biological stimulants outside of established parameters.

(11) Accidents/incidents involving Army chemical agent or research chemical agents listed below will be reported:

(a) The theft, loss, recovery, suspected theft, inventory shortage/overage, wrongful disposition, and unauthorized use and/or destruction of Army chemical agents or Army research chemical agent.

(b) Attempts to steal or divert Army chemical agents or Army research chemicals outside of physical security controls.

(c) Actual or attempted housebreaking or unauthorized access at an Army chemical facility or laboratory.

(d) Significant or disabling damage to an Army chemical facility.

(e) Confirmed or potential release of chemical agents to the environment.

(f) Mishaps which result in observable or known occupational exposures to Army chemical agents due to failure of personal protective equipment (PPE) to provide protection (such as malfunctions, improper, or inadequate use of PPE).

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

(h) Other Army chemical or Army research chemical agent incidents not identified above that the commander determines to be of immediate concern to HQDA based upon the nature, gravity, potential for adverse publicity, or potential consequences of the incident.

(12) Theft, suspected theft, wrongful appropriation, or willful destruction of Government property or appropriated funds valued at more than \$100,000.

(13) Theft, suspected theft, negligence, or conflict of interest involving Government non-appropriated funds or property valued at more than \$100,000.

(14) Racially or ethnically motivated criminal acts.

(15) Loss, theft, wrongful disposition, willful destruction, or mismanagement of the following:

(a) Evidence.

(b) Sensitive items, other than arms and ammunition, identified by Controlled Inventory Item Code 1-6, 8, 9, Q, R, or Y (see [AR 710-2](#)).

(c) Controlled cryptographic items.

(d) Drugs identified in the Comprehensive Drug Abuse Prevention and Control Act of 1970 as Schedules I, II, III, IV, and V controlled substances. Schedule II - V drugs are Government-controlled medical substances and are identified as R and Q controlled medical items in the Federal Supply Catalog. Schedule I drugs, as identified in the Act, are only used by DOD for research, and are not available through the supply system.

(16) Wrongful possession, manufacture, or distribution of controlled substances, to include narcotics, drugs, or marijuana in the quantities listed below:

- Cocaine, 100 grams or more.

TRADOC Reg 1-8

- Marijuana, 1000 grams or more.
- Hashish, 1000 grams or more.
- Heroin, 100 grams or more.
- Methamphetamines or barbiturates, 100 grams or more.
- LSD, 6 grams or more.
- PCP, 100 grams or more.

For narcotics and dangerous drugs not listed, use quantities for like substances listed above.

(17) Significant violations of Army standards of conduct, to include bribery, conflict of interest, graft, or acceptance of gratuities by Soldiers, DA, or nonappropriated fund employees.

(18) Incidents involving prisoners or detainees of Army confinement or correctional facilities to include escape from confinement or custody, disturbances which require the use of force, wounding, or serious injury to a prisoner, and all prisoner deaths.

(19) Theft, loss, suspected theft, unaccounted or recovered arms, ammunition, and explosives (AA&E) in the following quantities:

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

(b) Any machine gun or automatic fire weapon.

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

(d) Any explosives, to include demolition explosives (for example, detonation cord, blocks of explosives (C-4), and so on).

(e) One or more semiautomatic or manually operated firearms.

(f) Five or more rounds of ammunition greater than .50 caliber.

(g) 1,000 or more rounds of .50 caliber or smaller ammunition.

(h) Actual or attempted break-ins of arms rooms or storage areas for AA&E.

(i) Armed robbery or attempted armed robbery of AA&E.

(j) Any evidence of trafficking of AA&E, such as bartering for narcotics or any other thing of value, to include taking AA&E across international borders, regardless of the quantity of AA&E involved.

(20) Aggravated arson.

(21) All deaths occurring on TRADOC installations, except the death of a Family member or DA civilian which occurs due to natural causes in a medical facility (that is, pre-existing illnesses, disease, or medical condition). Deaths of TRADOC Soldiers occurring off military installations. All deaths of TRADOC Soldier's Family members and TRADOC DA civilians occurring off the installation that are deemed "not by natural causes" or "not under doctor's care." If cause of death is undetermined, complete the OPREP and update as soon as possible. Next of kin notifications, use of seatbelt/PPE, and alcohol/drug use will be included in the initial OPREP or updated accordingly in subsequent OPREPs.

(22) Kidnapping.

(23) Major fires or natural disasters involving death, serious injury, property damage in excess of \$250,000 (see additional reporting requirements in [AR 420-91](#)), or damage that seriously degrades unit operational or training capabilities.

(24) Group breaches of discipline involving 10 or more persons who collectively act to defy authority.

(25) Training and troop movement accidents resulting in serious injury or death.

(26) Maltreatment of Soldiers or DA civilians to include assaults, abuse, or exploitation where the offender has a trainer, supervisor, or cadre-trainee relationship with the victim, regardless of whether they are members of the same organization. Instances of consensual sex are not reportable unless other considerations such as sexual harassment or adverse publicity are involved.

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

(28) Actual or alleged incidents of child abuse which takes place within an Army organizational setting or facility (for example, child development center, youth activities center, military treatment facility, gymnasium, and so on) or an Army sponsored or sanctioned activity (for example, quarters-based Family child care home, youth sports or recreation activities, field trips, and so on).

(29) Serious child injury or death, not resulting from child abuse, while the child is in the Army's care at a nonmedical facility (that is, child development center, quarters-based Family child care home, youth activities center, and so on) or within an Army sponsored or sanctioned activity. This paragraph does not apply to sports injuries related to, or potentially inherent in, a youth activity or event.

(30) Serious domestic violence incidents (unrestricted reporting only). This report will include whether the Soldier was deployed within the past year leading up to the incident.

(31) Incidents involving firearms that cause injury or death.

TRADOC Reg 1-8

(32) Federal crimes reportable under [AR 381-10](#), when they meet reporting criteria.

(33) Serious injury or life-threatening injury to TRADOC Soldier, Family member, or DA civilian that creates a danger of loss of life, limb, or eyesight.

(34) Serious crime (that is, aggravated assault, sexual assault, larceny exceeding \$50,000, and murder or attempted murder) on or off the installation committed by or against a TRADOC Soldier, Family member, or DA civilian.

(35) Significant environmental injury to TRADOC Soldiers, Family members, or DA civilians 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.

(36) Communicable illnesses that exceed the expected baseline for those illnesses and unusual illnesses, such as H1N1 or Avian influenza. Consult with the local medical treatment facility.

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

(38) 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.

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

(a) 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.

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

(40) Command, control, communications, and computers (C4) outages/information systems intrusions/PII. All installation operation centers and TRADOC activities will report all

planned and unplanned degradations of C4 capabilities (as defined in [paragraph F-1](#)). A significant C4 degradation is:

(a) The loss of 50 percent or greater of a specific communications capability listed in paragraph F-1 lasting longer than 2 hours.

(b) Any degradation that results in a significant negative impact on the ability of the senior leader of a TRADOC activity (see [figure F-1](#)) to exercise command and control.

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

(42) All personnel will report all potential or malicious information system incidents or events. Incidents may result from accidental or deliberate actions on the part of a user or external influence. Information system incidents or events to be reported are defined in [AR 25-2](#), para 4-21.

(43) Report every PII breach. This applies to all Soldiers and civilian personnel assigned, attached, detailed, or on temporary duty with TRADOC organizations that control or collect PII. See paragraph [3-1e](#).

(a) 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.

(b) 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 othe 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 (IAW) [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.

(44) Trainee abuse, platoon sergeant, and drill sergeant misconduct.

(a) Allegations of trainee abuse as defined in [TRADOC Reg 350-6](#), paragraph 2-6 (any improper or unlawful physical, verbal, or sexual act against a trainee; does not include acts

TRADOC Reg 1-8

involving a trainee against trainee). However, if the credibility of the allegation can be quickly assessed (within 2 hours) and the command considers it not credible, an OPREP is not required. The noncredible allegation will be recorded and kept on file at the unit.

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

(45) 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.

(46) Environmental accidents or incidents at an installation with a TRADOC SC that result in:

(a) 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).

(b) 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.)

(47) 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 local commander or director of the radiological training facility that potentially impacts the mission.

(48) Change in threat or force protection condition.

(49) 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.

(50) Child abuse and domestic violence.

(a) Any alleged or actual incidents of child abuse that occur involving Army Family members or during an Army sponsored or sanctioned activity, whether on or off the installation, will be reported.

(b) Any incident of domestic violence against a Family member or person residing in the home or quarters of a military sponsor or as otherwise defined by state law, will be reported. 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. This paragraph applies to incidents of child abuse occurring within the family unit which involve the use of a weapon (for example, a firearm, knife, or other devices which will cause serious bodily injury), the victim suffers a broken limb, is sexually abused, is choked or strangled, or is admitted to the hospital because of injuries incurred during the incident.

(51) Any incident, event, or accident that may generate adverse publicity.

(52) Requests for support to civil authorities, to include those requesting "Immediate Response." For "Immediate Response" requests, also notify Army Watch within 2 hours. See [paragraph 3-1f](#).

(53) TRADOC's commander's critical information requirement is in accordance with the TRADOC Campaign Plan and is posted at the following link: <https://cac.tkeportal.army.mil/sites/g3/operations/default.aspx>. Look under orders, under OPORDS, under OPORD 09-008, FRAGO 01, appendix 1.

b. Any other incidents that the commander determines to be of concern to HQDA based on the nature, gravity, potential for adverse publicity, or potential consequences of the incident.

2-3. Suspicious activity report (SAR) reporting

Terrorist threat remains one of our Nation's most pervasive challenges. History has shown that DOD personnel, facilities, and activities make high-value terrorist targets, and no change is predicted for the future.

a. Suspicious activity shall be reported to servicing installation PMO/DES, USACIDC office, or 902nd Military Intelligence (MI) office for evaluation and submission to the Joint Terrorism Task Force.

b. Suspicious activity observed by TRADOC personnel or with a TRADOC nexus shall also be reported to HQ TRADOC using the TRADOC SAR.

c. The following suspicious activity must be reported:

(1) 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.

TRADOC Reg 1-8

(2) 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).

(3) 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.

(4) Expressed or implied threat. A threat to DOD personnel or threatened damage to or compromise of a DOD facility or infrastructure.

(5) 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).

(6) 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.

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

(8) 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.

(9) Sabotage, tampering, and/or vandalism. Damaging, manipulating, or defacing part of a DOD facility, infrastructure, or protected site.

(10) 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.

(11) 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.

(12) 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.

- (13) Weapons discovery. Discovery of weapons or explosives.
-

Chapter 3 Reporting Procedures

3-1. OPREP time requirements and means of reporting

a. Incidents will be reported to the TOC immediately upon discovery or notification at the installation. The reporting command will notify the TOC by the fastest means possible, either telephonic or e-mail. Call Defense Switched Network (DSN) 680-2256, commercial (757) 788-2256, e-mail to tradoc.eocwatch@conus.army.mil, or other reporting methods prescribed by the TOC. The TOC is operational 24 hours a day. Timeliness takes precedence over completeness for the initial report. Notification to the TOC by the reporting agency (installation operations center (IOC), command operations center, etc.) must be done immediately utilizing the methods stated. 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, facsimile (757) 788-2997 or DSN 680-2997, or other reporting methods prescribed by the TOC. 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 TOC within 4 hours of initial notification of the incident.*** OPREP numbering will be in concert with SIR conventions in [AR 190-45](#), figure 9-1. If initial OPREP requires follow up reporting, an "OPREP (Update)" will be submitted to provide information not available at the time of the original report or when more pertinent information, such as results of autopsy, identification of subject, and so on is developed, or in response to a request for more information from HQ TRADOC. "OPREP (Final)" reports will be submitted to close out "Initial" and/or "Update" OPREPs.

c. Use Unplanned C4 Outage Report ([figure F-2](#)) to notify TOC via e-mail to tradoc.eocwatch@conus.army.mil to report any unplanned, significant ([paragraph 2-2a\(40\)\(a\)](#)) degradation of C4 capabilities ([paragraph F-1](#)) IAW paragraph F-2. Use Planned C4 Outage Report ([figure F-2](#)) to notify TOC via e-mail to tradoc.eocwatch@conus.army.mil to report any planned significant ([paragraph 2-2a\(40\)\(a\)](#)) degradation of C4 capabilities ([paragraph F-1](#)) IAW [paragraph F-3](#).

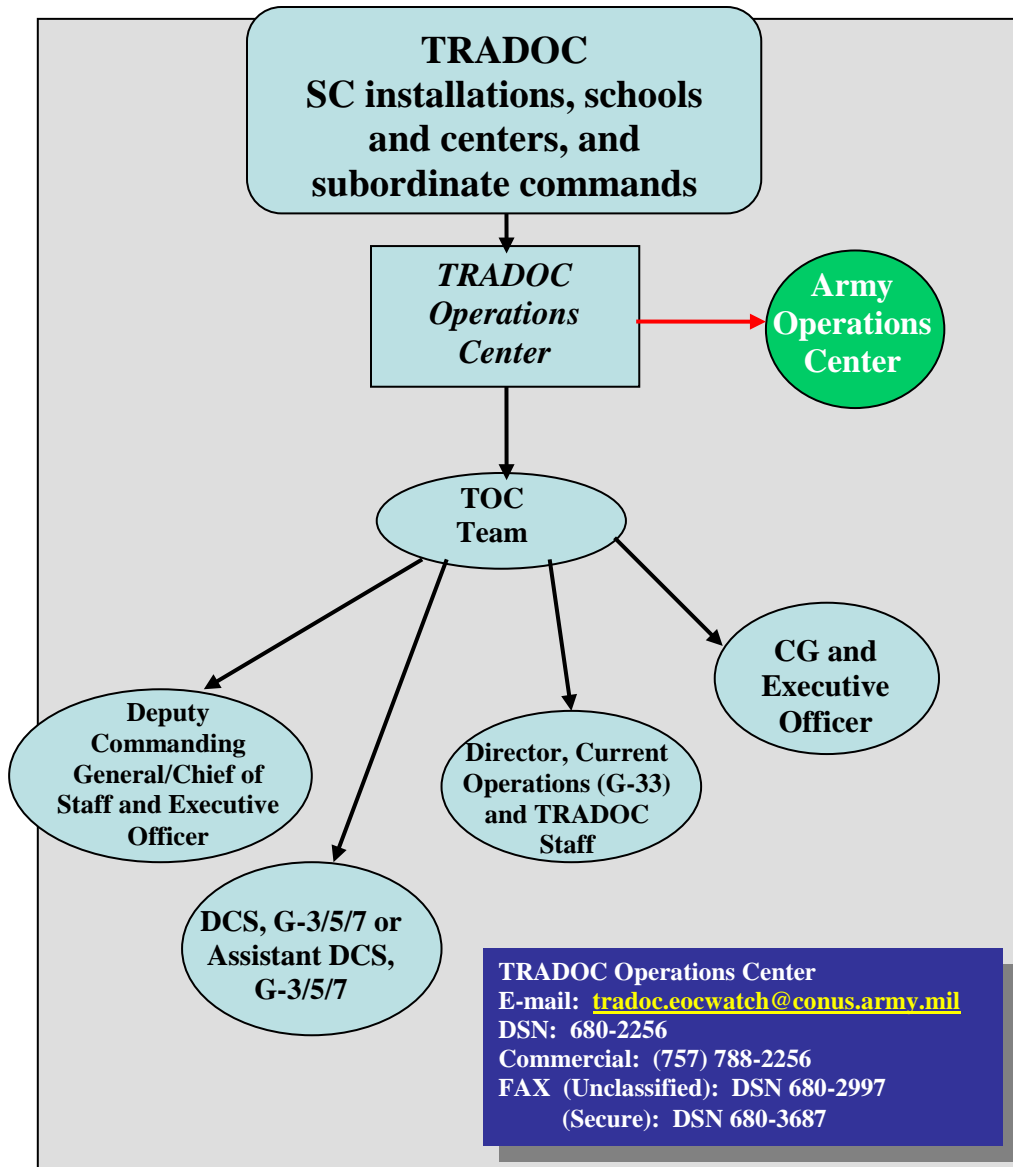


Figure 3-1. TRADOC OPREP Notification Process

d. An individual who suspects or observes an unusual or obvious incident or occurrence as defined in [paragraph 2-2a\(42\)](#) will:

(1) Cease all activities and keep the power on to the suspected information system.

(2) Immediately report the incident or occurrence to their Information Management Officer, systems administrator/network administrator, Information Assurance Security Officer, Information Assurance Manager (IAM), or supporting Directorate of Information Management/Network Enterprise Center.

(3) IAM will notify the IOC.

(4) IOC will submit Suspected or Observed Information System Incident Report (figure 3-2) to the TOC by e-mail to tradoc.eocwatch@conus.army.mil.

Suspected or Observed Information System Incident Report	
1. Installation:	_____
2. Activity:	_____
3. Type of Report (Initial, Follow-up, Final):	_____
4. Number/Type of Systems Affected:	
a. Workstations:	_____
b. File Servers:	_____
c. Print Servers:	_____
d. Web Servers:	_____
e. Others (Specify):	_____
5. Current System Status (Circle/bold/highlight all that apply):	
a. Disconnected from Network	
b. Log Files Collected	
c. System Rebuilt	
d. Other (Describe)	_____
6. Organization that detected suspected intrusion:	_____
7. Date/Time Suspected Intrusion Discovered - Local:	_____ Zulu: _____
8. Date/Time Intrusion Confirmed or Refuted - Local:	_____ Zulu: _____
9. POC Confirming/Refuting Intrusion:	
a. Name:	_____
b. Organization:	_____
c. Title:	_____
10. Reporting Activity POC Name:	_____
11. POC Phone - DSN:	_____ b. COMM: _____
12. POC Email:	_____
13. Date-Time Group of Report: Local:	_____ Zulu: _____
14. Additional Information:	

Figure 3-2. Example of Suspected or Observed Information System Incident Report

(5) TOC will forward this report to the HQ TRADOC, DCS, G-6 via e-mail to monr.atim@us.army.mil.

e. Use the DOD PII Breach Reporting Template at <https://www.rmda.army.mil/privacy/docs/DoD-PII-Incident-Reporting-Template.doc> to report every PII breach as defined in [paragraph 2-2a\(43\)](#). Commanders will ensure that PII breach procedures are followed and delegate execution to the supervisory level required ensuring compliance of all PII breach reporting and notification requirements.

(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/>. If computer access is unavailable, PII incidents can be reported to US-CERT by calling (703) 235-5110 which is monitored 24/7. US-CERT will e-mail the individual submitting the report a report incident number. Include the US-CERT report incident number on the DOD PII Breach Reporting Template.

(2) Complete and submit the initial OPREP message IAW [paragraph 3-1b](#) and include the completed <https://www.rmda.army.mil/privacy/docs/DoD-PII-Incident-Reporting-Template.doc> in the submission. The TOC will then forward the message to the TRADOC Office of the G-6 for processing to the Department of Army Privacy Office (pii.reporting@us.army.mil).

TRADOC Reg 1-8

(3) Alert the public affairs office for potential publicity.

(4) Complete notification to individuals considered at high risk for identity theft using the five factors to consider when assessing the likelihood of risk or harm IAW [appendix D](#).

f. Reporting installations will prepare and forward an initial OPREP for the following situation: 1) any request for support to civil authorities prior to providing support; 2) "immediate response" requests from civil authorities. Request for support from civil authorities require approval before any support can be provided, unless the local commander exercises 'immediate response' authority. For "immediate response" requests, also notify Army Watch through the TOC within 2 hours of the decision to provide "immediate response" assistance. This reporting requirement must be followed whether or not the assistance is provided according to a mutual support agreement.

3-2. SAR time requirements and means of reporting

a. Submit written SARs to the TOC within 4 hours of the incident in the SAR format. Telephonically notify the TOC 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 TOC IAW [paragraph 3-1a](#).

b. Installations will provide a complete SAR within 4 hours of the incident. When written or electronic reports are used, installations must call the TOC 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 TOC.

(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 For Official Use Only (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 HIPAA.

3-4. Required information

a. The OPREP report format is located in [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 [appendix B](#)).

3-5. Parallel report

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

TRADOC Reg 1-8

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 360-1

Public Affairs

AR 380-13

Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

AR 420-1

Army Facilities Management

DA Pam 600-24

Suicide Prevention and Psychological Autopsy

TRADOC Reg 350-6

Enlisted Initial Entry Training (IET) Policies and Administration

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.

AR 11-2

Management Control

AR 40-5
Preventive Medicine

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

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

DA Form 2028
Recommended Changes to Publications and Blank Forms

TRADOC Reg 1-8

Appendix B OPREP Report Form

B-1. OPREP report

As prescribed by [paragraph 3-1](#), submit an OPREP report for each incident.

B-2. OPREP report format example

See figure B-1 for the OPREP report format example.

From: CDRUSAICS Ft Benning GA//OFC SYMBOL//
TO: CDRUSATRADOC Ft Monroe VA//ATTG-OPA
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 (for death of Soldier, reports pay grade of E4 and below and list any enlistment waiver(s) received in order to enter military)
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

Figure B-1. Operations report format example

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 07, PV2 Doe went into massive renal failure and died.

8. Remarks:

- a. Next of Kin Notification: Yes, parents
- 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 70s
- 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.

Figure B-1. Operations report format example, continued

TRADOC Reg 1-8

Appendix C TRADOC SAR Format

C-1. TRADOC suspicious activity report

As prescribed in [paragraph 3-2](#), submit a SAR report for each incident.

C-2. TRADOC suspicious activity report format example

See figure C-1 for the SAR report format example.

TRADOC 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)

a. 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).

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, handdrawn 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.

Figure C-1. SAR report format example

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; 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 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, PMO, local law enforcement, etc.)

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

Figure C-1. SAR report format example, continued

TRADOC Reg 1-8

Appendix D

PII Breach Reporting Template, Notification, Remedial Actions, and Risk Analysis

D-1. DOD PII Breach Reporting Template

Individuals will use the DOD PII Breach Reporting Template to report every PII breach IAW paragraphs [2-2a](#) and [3-1e](#). See the DOD PII Breach Report Template with instructions on how to complete the template at <https://www.rmda.army.mil/privacy/docs/DoD-PII-Incident-Reporting-Template.doc>.

D-2. Report updates

Report updates will be made by:

a. Individuals will complete report updates to initial PII breach reports to ensure a complete report is filed. For example, complete a reporting update and include:

(1) The number of individuals affected by the breach is now known (it was reported as unknown on the initial report).

(2) The date the notification letters were mailed to affected individuals.

(3) Action taken against the Soldier.

b. The appropriate unit information assurance officer will report an incident involving possible compromise of Army networks to the appropriate regional computer emergency response team.

D-3. Notification procedures

Notification procedures to affected individuals deemed at high risk of identity theft.

a. The TRADOC organization that had responsibility to control access to the compromised PII must notify affected individuals deemed at high risk of identity theft, see table D-1, for the identity risk level. Coordinate with the local staff judge advocate and public affairs office (as applicable) prior to sending the notification letter. At a minimum, advise the individuals of the following: specific data involved; circumstances surrounding the loss, theft, or compromise; a statement as to whether the information was protected; for example, encrypted; and protective actions the individual can take to minimize their risk.

Table D-1
PII risk assessment model

Factor	Risk Determination	Comments
1. What is the nature of the data elements breached? What PII was involved?		
a. Name only	Low	Consideration needs to be given to unique names; those where only one or only a few in the population may have or those that could readily identify an individual, such as a public figure.
b. Name plus one more personal identifier (not SSN, medical, or financial)	Moderate	Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual.
c. SSN	High	
d. Name plus SSN	High	
e. Name plus medical or financial data	High	
2. Number of individuals affected		The number of individuals involved is a determining factor in how notifications are made, not whether they are made.
3. What is the likelihood the information is accessible and usable? What level of protection applied to this information?		
a. Encryption (FIPS 140-2)	Low	
b. Password	Moderate/ High	Moderate/High determined in relationship to category of data in number 1.
c. Not encrypted	High	
4. Likelihood the breach may lead to harm	High/ Moderate/ Low	Determining likelihood depends on the manner of the breach and the type(s) of data involved
5. Ability of the organization to mitigate the risk of harm		
a. Loss		Evidence exists that PII has been lost; no longer under DOD control
b. Theft		Evidence shows that PII has been stolen and could possibility be used to commit identify theft?
c. Compromise		
(1) Compromise with DOD control	Low/High	No evidence of malicious intent or evidence or possibility of malicious intent
(2) Compromise beyond DOD control	High	Possibility that PII could be used with malicious intent or to commit identity theft.

b. The TRADOC command/activity responsible for safeguarding the PII at the time of the incident must notify the affected individuals as soon as possible, but not later than 10 days after the loss or compromise of PII is discovered. Low/moderate/high risk or harm of identity theft is determined, and the decision whether notification of individuals is made rests with the head of the TRADOC command/activity where the breach occurred; however, all determinations of high risk or harm require notification. Commanders/directors will use the five factors to analyze the identity theft risk in [paragraph D-5](#) and risk assessment model in table D-1. When the TRADOC command/activity where the incident occurred is unknown, by default the responsibility for

TRADOC Reg 1-8

reporting the incident and notification of affected individuals lies with the originator of the document or information. Notification should be made by an individual at a senior level (such as, commander or director) to reinforce to impacted individuals the seriousness of the incident. Coordinate with the local staff judge advocate prior to sending the notification letter. At a minimum, advise the individuals of the following: specific data involved; circumstances surrounding the loss, theft, or compromise; a statement as to whether the information was protected; for example, encrypted; and protective actions the individual can take to minimize their risk. A sample notification letter is available at <https://www.rmda.army.mil/privacy/docs/SampleNotificationLetter.pdf>.

c. When the sender is not acquainted with the affected individuals, the commander/director will take precautions to alleviate unnecessary heartache caused by mass notification mailings being unknowingly addressed to deceased Soldiers. Prior to mailing or e-mailing mass notifications, the sender must ensure that all individuals receiving the notification are NOT named in the weekly death file produced by the Defense Manpower Data Center and NOT named in the up-to-date list of decedents produced by the Casualty and Mortuary Affairs Operations Center by e-mailing the mass mailing recipient list to COCOPNS@conus.army.mil for confirmation.

D-4. Remedial actions

Commanders and supervisors will ensure the appropriate remedial action(s) are taken when PII is lost or compromised. At a minimum, if PII is lost as a result of negligence or failure to follow established procedures, the individual(s) responsible will receive counseling and additional training reminding them of the importance of safeguarding PII. Additional remedial actions may include prompt removal of authority to access information or systems from individuals who demonstrate a pattern of error in safeguarding PII, as well as other administrative or disciplinary actions as determined appropriate by the commander or supervisor.

D-5. Identity theft risk analysis

Commanders/directors will consider these five factors when assessing the likelihood of risk and/or harm. It is difficult to characterize data elements as creating low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

a. Nature of the data elements breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. For example, theft of a database containing individuals' names in conjunction with SSNs, and/or dates of birth may pose a high level of risk or harm, while a theft of a database containing only names of individuals may pose a lower risk, depending on its context.

b. Number of individuals affected. The magnitude of the number of affected individuals may dictate the method (should) you choose for providing notification, but should not be the only determining factor for whether an agency should provide notification.

c. Likelihood the information is accessible and usable. Upon learning of a breach, agencies should assess the likelihood PII will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

(1) Depending on a number of physical, technological, and procedural safeguards employed by the agency, the fact that information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. If the information is properly protected by encryption, for example, the risk of compromise may be low to nonexistent. In this context, proper protection means encryption has been validated by the National Institute of Standards and Technology (NIST).

(2) Agencies will first need to assess whether the breach involving PII is at a low, moderate, or high risk of being used by unauthorized persons to cause harm to an individual or group of individuals. The assessment should be guided by NIST security standards and guidance. Other considerations may include the likelihood any unauthorized individuals will know the value of the information and either use or sell the information to others.

d. Likelihood the breach may lead to harm.

(1) Broad reach of potential harm. The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Additionally, agencies should consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

(2) Likelihood harm will occur. The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the types(s) of data involved in the incident. SSNs and account information are useful for committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other PII, the loss may also pose a significant risk of harm if, for example, it appears on a list of patients at a clinic for treatment of a contagious disease.

e. Ability of the agency to mitigate risk of harm. Within an automated information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of personal information and patterns of suspicious behavior should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

TRADOC Reg 1-8

f. All breaches of PII, whether actual or suspected, require notification to US-CERT. Low and moderate risk/harm determinations and the decision whether notification of the individuals is made, rest with the head of the TRADOC organization where the breach occurred. All determinations of high risk/harm require notification. TRADOC organizations are to thoroughly document the circumstances of all breaches of PII and the decisions made relative to the factors above in reaching their decision to notify or not notify individuals.

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 5 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 TOC immediately upon discovery or notification at the installation, HQ, United States Army Cadet Command (USACC), or HQ, United States Army Recruiting Command (USAREC) level?
- c. Are initial written OPREPs sent to TOC 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 TOC 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 TOC?
- g. Are SARs used IAW [paragraph 2-3](#) of this regulation?
- h. Are SARs submitted to the TOC 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.

TRADOC Reg 1-8

E-6. Comments

Help to make this a better tool for evaluating management controls. Submit comments directly to Director, Current Operations (G-33), DCS, G-3/5/7 (ATTG-OPA), 5 Fenwick Road, Fort Monroe, VA 23651.

Appendix F C4 Degradation Reporting

F-1. C4 degradation

All installation operation centers and TRADOC activities will report all planned and unplanned degradations of the following C4 capabilities:

- a. Telephone system/service (separate reporting not required for facsimile service).
- b. E-mail services (SIPRNet or NIPRNet).
- c. NIPRNet service.
- d. SIPRNet service.
- e. Installation video teleconference studio.
- f. Iridium telephone.
- g. IOC global system for mobile communications cellular telephone.

F-2. Unplanned C4 degradation within IOCs and/or TRADOC activities

a. IOC:

(1) Notify TOC by e-mail to tradoc.eocwatch@conus.army.mil to report any unplanned, significant ([paragraph 2-2a\(40\)\(a\)](#)) degradation of C4 capabilities ([paragraph F-1](#)). Identify scope of outage, operational impact, reason if known, and estimated time of repair (determine if outage will last for longer than 2 hours).

(2) If outage will last for more than 2 hours, submit Unplanned C4 Outage Report (figure F-1) to TOC via e-mail to tradoc.eocwatch@conus.army.mil. Submit report within 4 hours of initial telephone or e-mail notification to TOC.

b. TOC:

(1) Send reported degradation to HQ TRADOC, Deputy Chief of Staff, G-6, via e-mail to monr.atim@us.army.mil.

(2) Place information in the Daily Event Summary.

Unplanned C4 Outage Report	
1. Installation:	_____
2. Activity:	_____
3. Type of Report (Initial, Follow-up, Final):	_____
4. C4 Capability:	_____
5. Scope of Outage:	_____
6. Time Outage Discovered - Local:	_____ Zulu: _____
7. Time Outage Corrected - Local:	_____ Zulu: _____
8. Reason for Outage:	_____

9. Alternate Communications Means:	_____

10. Reporting Activity POC Name:	_____
11. POC Phone - DSN:	_____ b. COMM: _____
12. POC Email:	_____
13. Date-Time Group of Report: Local:	_____ Zulu: _____
14. Additional Information:	

Figure F-1. Unplanned C4 outage report

F-3. Planned C4 degradations within IOCs and/or TRADOC activities

a. IOC:

(1) Submit Planned C4 Outage Report (figure F-2) to report any planned significant [paragraph 2-2a\(40\)\(a\)](#) degradation of C4 capabilities ([paragraph F-1](#)).

Planned C4 Outage Report	
1. Installation:	_____
2. C4 Capability:	_____
3. Scope of Outage:	_____
4. Time Outage Discovered - Local:	_____ Zulu: _____
5. Reason for Outage:	_____

6. Alternate Communications Means:	_____

7. Reporting Activity POC Name:	_____
8. POC Phone - DSN:	_____ b. COMM: _____
9. POC Email:	_____
10. Date-Time Group of Report: Local:	_____ Zulu: _____
11. Additional Information:	

Figure F-2. Planned C4 outage report

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
CoE	Center of Excellence
CPMD	Command Provost Marshall Directorate
CPR	cardiopulmonary resuscitation
DA	Department of the Army
DCS	deputy chief of staff
DES	Director of Emergency Services
DOD	Department of Defense
DSN	Defense Switched Network
EMS	Emergency Medical Services
EOC	emergency operations center
FOUO	For Official Use Only
HIPAA	Health Insurance Portability and Accountability Act
HRC	Human Resource Command
HQ	headquarters
HQDA	Headquarters, Department of the Army
IAM	Information assurance manager
IAW	in accordance with
IOC	installation operations center
MI	military intelligence
NIST	National Institute of Standards and Technology
OPREP	operations report
PII	personally identifiable information
PMO	provost marshal office
PPE	personal protective equipment
SAR	Suspicious Activity Report
SIR	serious incident report
SC	senior commander
SSN	social security number
TOC	U.S. Army Training and Doctrine Command Operations Center
TRADOC	U.S. Army Training and Doctrine Command
USAAC	United States Army Accessions Command
USACC	United States Army Cadet Command
USACIDC	United States Army Criminal Investigation Command
USAREC	United States Army Recruiting Command
US-CERT	United States Computer Emergency Readiness Team

Section II

Terms

Chemical agent

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

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.