

Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Eustis, Virginia 23604

*TRADOC Regulation 1-8

11 August 2017

Administration

U.S. ARMY TRAINING AND DOCTRINE COMMAND OPERATIONS REPORTING

DAVID G. PERKINS
General, U.S. Army
Commanding



RICHARD A. DAVIS
Senior Executive
Deputy Chief of Staff, G-6

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

Summary. This regulation prescribes the operational reporting of significant incidents to Headquarters (HQ), United States Army Training and Doctrine Command (TRADOC).

Applicability. This regulation applies to all elements of TRADOC, to include HQ TRADOC installations where a TRADOC officer is the senior commander, 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 regulation that are consistent with controlling laws 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 02 December 2014.

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), 950 Jefferson Avenue, Fort Eustis, VA 23604.

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), 950 Jefferson Avenue, Fort Eustis, VA 23604. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal).

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

Summary of Change

TRADOC Regulation 1-8

U.S. Army Training and Doctrine Command Operations Reporting

This rapid action revision, dated 11 August 2017-

- o Updates or removes from Category III reportable events and incidents for clarity and to avoid redundancies (para 2-2).
- o Adds specific reportable events and incidents with the source documents (para 2-2).
- o Combines United States Army Training and Doctrine Command Category III reporting requirements (para 2-2).
- o Modifies reporting of privately owned weapons (para 2-3c(13)).
- o Clarifies reporting requirements (para 3-1a).
- o Adds new Department of Defense Directive 5400.11, dated October 29, 2014, and Headquarters, Department of the Army Commander's Critical Information Requirements (app A).
- o In the Glossary, Section II, Terms, added two definitions for clarity of reporting.

Contents

	Page
Chapter 1 Introduction	5
1-1. Purpose	5
1-2. References	5
1-3. Explanation of abbreviations and terms	5
1-4. Responsibilities.....	5
Chapter 2 Reporting Policy.....	6
2-1. Policy	6
2-2. Reportable events and incidents	6
2-3. Suspicious activity report (SAR) reporting	9
Chapter 3 Reporting Procedures	11
3-1. Time requirements and means/mode of reporting	11
3-2. SAR time requirements and means of reporting	14
3-3. Handling of reports	15
3-4. Required information.....	15
3-5. Parallel report	15
Appendix A References	16
Appendix B Serious incident report (SIR) Report Form	17
Appendix C United States (U.S.) Training and Doctrine Command (TRADOC) SAR Format .	19
Appendix D Personally identifiable information (PII) Breach Reporting Template, Notification, Remedial Actions, and Risk Analysis	20
Appendix E Management Control Checklist	26
Appendix F Command, control, communications, and computers (C4) Degradation Reporting	28
Glossary	30

Figure List

Figure 3-1. TRADOC SIR Notification Process.....	11
Figure 3-2. Example of Suspected or Observed Information System Incident Report	13
Figure B-1. SIR format example.....	19
Figure C-1. SAR report format example.....	20
Figure D-1. Sample Department of Defense (DD) Form 2959	23
Figure D-2. Sample TRADOC center/activity Breach Report PII Flowchart	25
Figure F-1. Unplanned C4 outage report	29
Figure F-2. Planned C4 outage report.....	30

This page intentionally left blank

Chapter 1

Introduction

1-1. Purpose

To establish policy and procedures for the reporting of significant incidents involving United States (U.S.) Army Training and Doctrine Command (TRADOC) senior commander (SC) installations, TRADOC schools and centers of excellence, 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 this process 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 analysis, develop mitigation policies, and to integrate the data into the appropriate forums to refine procedures and mitigate incidents.

1-2. References

The primary sources for reporting requirements are the TRADOC Commander's Critical Information Requirements (CCIRs), Serious Incident Reports (SIRs) (Army Regulation (AR) 190-45) and Suspicious Activity Reports (SARs). Publications prescribing requirements and processing 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, school and center commandants/commanders, subordinate commanders, and TRADOC activity, unit, and HQ TRADOC element personnel will ensure the policies and procedures of this regulation are implemented in their organizations.

a. TRADOC SCs, commandants/commanders, activities, units, and subordinate element personnel are responsible for reporting the events and incidents as defined in Chapter 2, as well as any other matter that commanders determine to be of concern to the Commanding General (CG), TRADOC.

b. 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 SIRs.

c. DCS, G-3/5/7, Director, Protection Division (G-34) or a G-34 designated representative will analyze each SAR and ensure they are entered into eGuardian, if they meet the eGuardian criteria.

d. TRADOC Operations Center (TOC) is responsible for collecting, analyzing, and referring all SIRs and SARs to the Director, Current Operations (G-33), TRADOC leadership, and to appropriate HQ and staff sections, adjacent, and higher commands as appropriate. The TOC will receive reports, request follow-ups, and report incidents to TRADOC leadership.

e. 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. If in doubt, submit a SIR.

b. Reporting procedures outlined in this regulation do not replace the reporting procedures 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/Director of Emergency Services and/or U.S. Army Criminal Investigation Division Command (USACIDC) office for appropriate inquiry and investigation.

2-2. Reportable events and incidents

TRADOC SIRs are derived from multiple sources; however, primary sources are:

a. HQDA CCIRs as published and maintained by Department of the Army Management Office of Operations and Contingency Planning (DAMO-ODO).

b. TRADOC CCIRs as published in TRADOC Operation Orders and Fragmentary Orders.

c. AR 190-45 and SIRs per Chapters 8 & 9, CAT 1 & 2 reportable incidents.

d. Category (CAT) 3. The following are TRADOC specific requirements reportable as CAT 3 (this category was developed by TRADOC Emergency Operations Center and replaces what was previously known as “Additional CAT II”).

(1) Training use of riot control agent or chemical material stimulants outside of established parameters.

(2) Serious crime (that is, aggravated assault, any unrestricted sexual assault not covered under FFIRs, larceny exceeding \$50,000, and murder or attempted murder) on or off the installation committed by or against a TRADOC Soldier, dependent, DA Civilian, contractor, future Soldier, or contracted Senior Reserve Officer Training Corps (ROTC) Cadet. This also

applies to any Senior ROTC cadet while in training status. Additionally, all sexual assault cases are required to be entered into Defense Sexual Assault Incident Database (DSAID) upon notification and the DSAID number entered in the SIR line 13, or “Unknown” for each case entered.

(3) Significant environmental injury to a TRADOC Soldier, dependent, or DA Civilian 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.

(4) Communicable illnesses that exceed the expected baseline for those illnesses and unusual illnesses. Consult with the local medical treatment facility.

(5) 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, 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, Advanced Individual Training, and Officers Initial Entry Training) then indicate initial entry training status in the SIR summary of incident section. (See [DA Pamphlet \(DA Pam\) 600-24](#) for suicide prevention information).

(6) Aircraft accident or incident (Class B, C, and D). Any type of aircraft accident or incident that causes damage to aircraft or injury to personnel (manned or unmanned). Reporting requirements extend to tenant or transient aircraft from another service or command using TRADOC facilities or land in the geographic area of responsibility.

(7) Command, Control, Communications, and Computers (C4) outages. All installation operation centers and TRADOC activities will report planned and unplanned degradations of C4 capabilities (as defined in paragraph F-1). A reportable 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.

(8) Major installation utilities/interruptions that impact operations and training.

(9) Suspected or confirmed information system incidents or intrusions. Incidents or events to be reported are defined in AR 25-2, para 4-21.

(10) PII breaches. 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.

TRADOC Regulation 1-8

(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 other than authorized purpose have access or potential access to PII, whether physical or electronic. This includes, but is not limited to, posting PII on public-facing websites (except in the case of approved public affairs releases in accordance with [AR 360-1](#), paragraph 5-3); sending via e-mail to unauthorized recipients; providing hard copies to individuals without a need to know; loss of electronic devices or media storing PII (for example, laptops, thumb drives, compact discs, etc.); use by employees for unofficial business and all other unauthorized access to PII.

(11) Trainee abuse or platoon sergeant, drill sergeant, recruiter, ROTC/junior ROTC cadre misconduct.

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

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

(12) 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).

(13) Incidents/accidents involving international students and international staff 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.

(14) Any incident involving spillage of classified information. A spillage is classified information transferred over from secure internet protocol router network (SIPRNET) to non-secure internet protocol router network (NIPRNET), or other compromises of classified information to include electronic transfer, hard copy documents, or equipment. See AR 25-2 (para 4-21) and para 3-1g this document for more details.

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

2-3. Suspicious activity report (SAR) reporting

Suspicious activity reporting is established to provide a means to capture all-threats and suspicious activity against all TRADOC assets and creates a standardized reporting format adaptable for quick analysis and action.

a. Suspicious activity shall be reported to servicing installation provost marshal office/ Director of Emergency Services, USACIDC office, or 902nd Military Intelligence office for evaluation and entry into eGuardian, if they meet the eGuardian criteria. U.S. Army Cadet Command and U.S. Army Recruiting Command will report all suspicious activity to the Criminal Investigation Division analyst detailed to TRADOC G-34 for evaluation and entry into the eGuardian, if they meet the eGuardian criteria.

b. Suspicious activity observed by TRADOC personnel or involving TRADOC assets 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 that would cause a reasonable person to perceive a threat to DOD personnel, facilities, or forces in transit.

(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. Acts of vandalism committed by DOD civilian employees, Service members, or their dependents should not be reported as suspicious activity unless those acts relate to a pattern of criminal activity or otherwise would cause a reasonable person to perceive a threat to DoD personnel, facilities, or forces in transit.

(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) Discovery of weapons or explosives. The discovery of privately owned weapons and/or ammunition will be reported only if concluded to be suspicious in nature.

Chapter 3
Reporting Procedures

3-1. Time requirements and means/mode of reporting

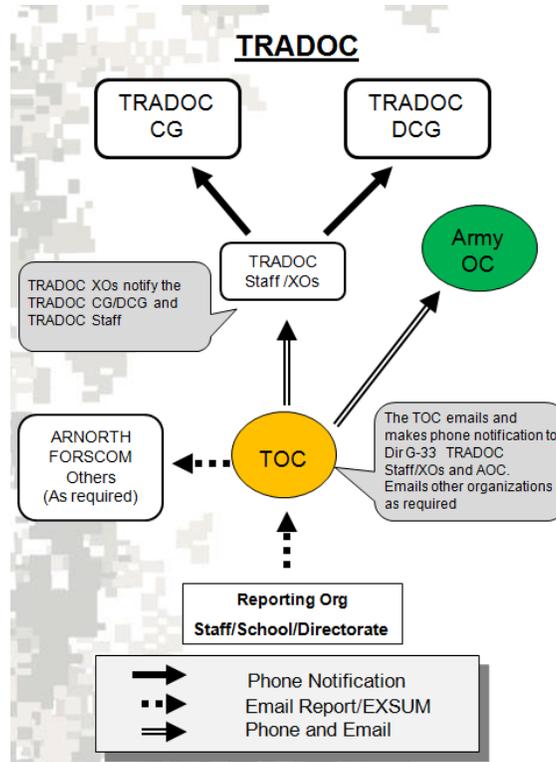


Figure 3-1. TRADOC SIR Notification Process

a. Incidents on TRADOC CDR’s CCIR designated as “ALL hours Call” and CAT #1 and #2 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, Electronic Reporting Portal (ERP) at <https://hq.tradoc.army.mil/sites/ERP/default.aspx> or encrypted e-mail. Call Defense Switched Network (DSN) 501-5096, commercial (757) 501-5096, e-mail to usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.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. See figure 3-1 for the TRADOC SIR notification process.

b. Regardless of immediate reporting mode, reporting installations, schools, or centers are required to submit a report to the TOC via the ERP in accordance with SIR reporting procedures in Chapter 9, AR 190-45. If the ERP is inoperable, reports will be submitted using format in

[appendix B](mailto:usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil), by encrypted e-mail to usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil, facsimile (757) 501-5122 or DSN 501-5122, or other reporting methods prescribed by this publication. Provide all the available information in the SIR summary block. Copy and paste the SIR summary block into the e-mail body, omitting all PII from the summary. Reporting entities will submit final reports for closeout.

c. Use Unplanned C4 Outage Report (figure F-1) to notify TOC via e-mail to usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil to report any unplanned, significant degradation of C4 capabilities in accordance with paragraph F-2. Use Planned C4 Outage Report (figure F-2) via e-mail to usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil to report any planned significant degradation of C4 capabilities in accordance with paragraph F-3.

d. 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. Personnel 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, or supporting Network Enterprise Center.
- (3) Information Assurance Manager will notify the Installation Operations Center (IOC).
- (4) IOC will submit Suspected or Observed Information System Incident Report (figure 3-2) to the TOC by e-mail to usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.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.

e. Report all incidents involving the actual or suspected breach/compromise of PII. This applies to all Soldiers and Civilian personnel assigned, attached, detailed, or on temporary duty with TRADOC organizations that control or collect PII. The command, activity, or unit that discovered a breach/compromise will make the initial notification to the TOC, and the affected command will report using the Department of Defense Form (DD Form) 2959 to the TOC and appropriate channels. 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://www.us-cert.gov/forms/report>. If computer access is unavailable, PII incidents can be reported to US-CERT by calling (888) 282-0870 which is monitored 24/7. US-CERT will provide two incident report numbers to be included on the [DD Form 2959](#), i.e., a US-CERT Number and a Internal Component Number.

(2) Complete and submit the initial SIR message in accordance with paragraph 3-1b and include the completed [DD Form 2959](#) in the submission to the TOC usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil. The TOC will then forward the message to the TRADOC Office of the G-6 for processing to the Department of Army Privacy Office.

(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 in accordance with Appendix D.

f. Reporting installations will prepare and forward an initial SIR for the following situation:

(1) Any request for support to civil authorities prior to providing support.

(2) "Immediate response" requests from civil authorities. Requests 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.

g. Commanders will report classified spillages within 24 hours of the initial incident. See [TRADOC DCG Memo, 26 Aug 13, SUBJECT: Classified Information Security Incident Reporting](#) for further information.

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 immediately upon discovery or notification of the suspicious activity. Classification of the initial SAR is unclassified. The reporting command will provide initial notification to the TOC in accordance with paragraph 3-1a.

b. 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).

c. 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.

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

3-3. Handling of reports

a. Due to the potentially sensitive nature of SIRs and SARs, all e-mails and reports will be marked at a minimum of 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 SIRs as it relates to the SIR incident. IOCs will not report unrelated patient health information in an SIR to a third party without the patient's consent in accordance with HIPAA.

3-4. Required information

a. The SIR report format is located in Appendix B. Reports will include all available, relevant facts. SIRs provided telephonically and via e-mail will identify individuals by rank, name, unit of assignment, and Army command. 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 SIR (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.

Appendix A References

Section I

Required Publications

ARs, DA Pams, and DA Forms are available at www.apd.army.mil. TRADOC publications and forms are available at <http://www.tradoc.army.mil/Publications.asp>.

[DoDD 5400.11-R, Department of Defense Privacy Program, OCT 29, 2014](#)

[HQDA CCIR, JUN 8, 2017](#)

AR 25-2 - Information Assurance

AR 190-45 - Law Enforcement Reporting

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 Regulation 350-6 - Enlisted Initial Entry Training (IET) Policies and Administration

[TRADOC DCG Memo, 26 Aug 13, SUBJECT: Classified Information Security Incident Reporting](#)

CCIRs as published under CG TRADOC orders.

Section II

Related Publications

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

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

Appendix B Serious incident report (SIR) Report Form

B-1. SIR report

As prescribed by paragraph 3-1, submit an SIR report for each incident.

B-2. SIR report format example

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

From: CDRMCoE Ft Benning GA//OFC SYMBOL//
TO: CDRUSATRADOC Ft Eustis VA//ATTG-OPA
usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil
Info: IMCOM Ops Ctr

1. Report Date & Time: 011100 July 14
2. Reporting Installation: Ft Benning GA
3. OPREP/SIR#: BENN011100JUL14-1
4. Subject: Doe, John
5. Status of Report: INITIAL (*Initial/Update/Final*)
6. Category: SIR Cat II (*CCIR, SIR Cat I, SIR Cat II, SIR Cat III, SAR*)
 - 7a. Type of Incident: Death/Loss of Life
 - 7b. Incident Sub-Cat 1: Death of a Soldier
 - 7c. Incident Sub-Cat 2:
8. Date & Time of Incident: 010730 July 14
9. Location of Incident: Ft Benning GA (On Post)
10. 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

TRADOC Regulation 1-8

(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.

11. Racial: No

12. 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*)

13a. Name of Subject Involved: Doe, John

13b. Subject's Rank/Title: PV2

13c(1). Subject's ACOM: TRADOC (*FORSCOM, INSCOM, MEDCOM, etc.*)

13c(2). Subject's Component: Active (*Active, Reserve, National Guard, Other, N/A, UNK*)

13c(3). Subject's Service: Army (*Army, Air Force, Navy, etc.*)

13d. Subject's SSN#: 123-45-6789

13e. Subject's Race: White

13f. Subject's Sex: Male

13g. Subject's Age: 18

13h. Subject's Position: Trainee (*Trainee, Cadre, Permanent Party, etc.*)

13i. Subject's Security Clearance: S-NAC (*Secret, S-NAC, TS, Interim, None, etc.*)

13j. Subject's Unit & Station: A Co, 2-29 IN (TRADOC)

13k. Subject's Duty Status: Present

14a. Name of Victim: N/A

14b. Victim's Rank/Title:

14c(1). Victim's ACOM:

14c(2). Victim's Component:

14c(3). Victim's Service:

14d. Victim's SSN#:

14e. Victim's Race:

14f. Victim's Sex:

14g. Victim's Age:

14h. Victim's Position:

14i. Victim's Security Clearance:

14j. Victim's Unit & Station:

14k. Victim's Duty Status:

15. NOK Notification: Yes, parents

16. Soldier Deployed within Last Year?: No

17. Were Seatbelts Worn?: N/A

18. Was Alcohol Involved?: No

19. Was PPG/E Worn?: N/A

20. Any Previous Medical History?: UNK

21. Were Combat Lifesavers Present?: Yes

22a. Was CPR Performed at the Scene?: No

22b. Date & Time CPR Started: N/A

22c. Date & Time 911 Called?: 010735 Jul 14

22d. Date & Time EMS Personnel Arrived on Scene: 010745 Jul 14

22e. Date & Time EMS Departed Scene En Route To Hospital: 010750 Jul 14

22f. Date & Time EMS Arrived at Hospital: 010800 Jul 14

22g. Date & Time Soldier Pronounced Dead: 010810 Jul 14

- 23a. Was anything different noticed about the Soldiers performance: Yes. Ungainly gait.
- 23b. If Yes (Please Explain):
- 24. Ages/Gender of Family Members: N/A
- 25a. Type of Training: One station unit training
- 25b. Phase of Training: 3d week
- 26. Weather Conditions at Time of Incident: Overcast, temp in low 70s
- 27. Other Factors Contributing to the Incident:
- 28. Publicity: None expected at this time
- 29. Commander Reporting: COL I.M. Short, COS
- 30. Point of Contact: SFC Dill, SDNCO, DSN 835-0000, BENN.DOT.EOC@benning.army.mil
- 31. Comments/Remarks: None
- 32. Downgrading Instructions: The FOUO protective marking may be removed on DDMMYYYY.

Figure B-1. SIR format example

Appendix C

United States (U.S.) Training and Doctrine Command (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, 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, but 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

Appendix D

Personally identifiable information (PII) Breach Reporting Template, Notification, Remedial Actions, and Risk Analysis

D-1. Department of Defense Form (DD Form) 2959

Personnel will use the DD Form 2959 to report every PII breach in accordance with paragraphs 2-2a and 3-1e. See Figures D-1 and D-2 for a sample of a completed DD Form 2959 and a sample TRADOC center/activity Breach Report PII Flow Chart. See the TRADOC Privacy Act/PII Reporting site at <http://www.tradoc.army.mil/PrivacyAct.asp>.

D-2. Report updates

Report updates will be made by the affected command:

a. Personnel 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 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. TRADOC must continue its efforts to promote a culture to continuously 'think privacy' and act swiftly to develop and implement effective breach mitigation plans, when necessary. Our challenge is that no two breaches of PII involve the exact same circumstances, personnel, systems, or information. A case-by-case analysis combined with the use of best judgment is required for effective breach management. The determination whether to notify individuals of a breach is based on an assessment of the likelihood that the individual will be harmed as a result of the breach and its impact. Harm includes embarrassment, inconvenience, financial loss, blackmail, identity theft, emotional distress and loss of self-esteem. See paragraph D-5 for the five factors should be weighed to assess the likely risk of harm.

b. A formal decision regarding whether to notify cannot be made until after each factor has been assessed. The decision to notify should not be based on one factor alone. For example, a breach involving SSNs makes that factor a high risk. However; SSNs may be stored on an encrypted, Common Access Card-enabled laptop to mitigate potential compromise which could lead to harm. Therefore, although one factor in this example (data elements) rates as a high likelihood of harm, after all factors are evaluated and considered, the overall likelihood of harm resulting from the breach is low given the technical safeguards in place. Generally, absent other factors, the TRADOC command/activity should not notify personnel of breaches that have a low overall likelihood of harm. TRADOC command/activity should remain cognizant of the effect that unnecessary notification may have on the public. Notification when there is little or no risk of harm might create unnecessary concern and confusion. Additionally, overzealous notifications resulting from notification criteria which are too strict could render all such notifications less effective because consumers could become numb to them and fail to act when risks are truly significant.

c. 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.

d. When the TRADOC command/activity where the incident occurred is unknown, by default the responsibility for reporting the incident and notification of affected individuals lies with the originator of the document or information. Notification to impacted individuals 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>.

BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (PII) REPORT			
INITIAL REPORT	Date: (MM/DD/YYYY) 05092013	X	UPDATED REPORT
			Date: (MM/DD/YYYY) 05142013
			AFTER ACTION REPORT
			Date: (MM/DD/YYYY)
1. GENERAL INFORMATION			
a. DATE OF BREACH (MM/DD/YYYY) 05082013	b. DATE BREACH DISCOVERED (MM/DD/YYYY) 05082013	c. DATE REPORTED TO US-CERT (MM/DD/YYYY) 05092013	d. US-CERT NUMBER USCERT-2014XXXXXXXX or INC
e. COMPONENT INTERNAL TRACKING NUMBER (if applicable) SIR 14-XXXX	f. BREACH INVOLVED (Click to select) Info dissemination	g. TYPE OF BREACH (Click to select) Compromise	h. CAUSE OF BREACH (Click to select) Failure to follow policy
i. COMPONENT (Click to select) Department of the Army		j. OFFICE NAME TRADOC G-6 on behalf of CASCOM G-6	
POINT OF CONTACT FOR FURTHER INFORMATION:			
k. FIRST NAME Miss Ing	l. LAST NAME Records	m. RANK/GRADE AND TITLE GS-11 Records Administrator	
n. DUTY E-MAIL ADDRESS miss.ing.records.civ@mail.mil		o. DUTY TELEPHONE NUMBER 757-501-XXXX	
MAILING ADDRESS:			
p. ADDRESS DEPUTY CHIEF OF STAFF G-6 661 SHEPPARD PLACE (ATIM-II)		q. CITY Fort Eustis	
		r. STATE Virginia	s. ZIP CODE 23604-5733
2.a. DESCRIPTION OF BREACH (Up to 150 words, bullet format acceptable). NOTE: Do NOT include PII or Classified Information.			
Initial: CASCOM G6 was notified of a PII Breach that occurred on AKO. The Army Web Risk Assessment Cell found a file that was uploaded to AKO by a Fort Lee (TRADOC) user that contained PII. The Army Web Risk Assessment cell generated USCERT 2014-XXXXXXXX for the AKO incident.			
Update: Upon further investigation, it was discovered that the file in question was originally sent out in an e-mail. That e-mail was also forwarded out more than once to numerous Army personnel, and some of those personnel do not have a need-to-know the information in the record. CASCOM G-6 generated USCERT-2014XXXXXXXX for the e-mails containing the PII information.			
2.b. ACTIONS TAKEN IN RESPONSE TO BREACH, TO INCLUDE ACTIONS TAKEN TO PREVENT RECURRENCE AND LESSONS LEARNED (Up to 150 words, bullet format acceptable). NOTE: Do NOT include PII or Classified Information.			
Initial:			
- Chain of command notified.			
- US-CERT report filed.			
- Initial SIR prepared.			
- DD Form 2959 prepared.			
Update:			
- Identification of PII in numerous e-mail accounts.			
- Chain of command notified of data collection results.			
- NEC-LEE IAM informed of data collection results.			

DD FORM 2959, FEB 2013

Adobe Designer 9.0

Figure D-1. Sample [Department of Defense \(DD\) Form 2959](#)

3.a. NUMBER OF INDIVIDUALS AFFECTED (1) Contractors (2) DoD Civilian Personnel (3) Military Active Duty Personnel (4) Military Family Members (5) Military Reservists (6) Military Retirees (7) National Guard (8) Other (Specify):	b. WERE AFFECTED INDIVIDUALS NOTIFIED? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No (2) If Yes, notification date (MM/DD/YYYY) 05152013 (4) If notification will not be made, explain why, or if number of individuals notified differs from total number of individuals affected, explain why: (5) If applicable, was credit monitoring offered? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	(1) If Yes, were they notified within 10 working days? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No (3) If Yes, number of individuals notified: 12
4. PERSONALLY IDENTIFIABLE INFORMATION (PII) INVOLVED IN THIS BREACH (X all types that apply)		
<input checked="" type="checkbox"/> (1) Names <input checked="" type="checkbox"/> (2) Social Security Numbers <input checked="" type="checkbox"/> (3) Dates of Birth <input type="checkbox"/> (4) Protected Health Information (PHI) <input type="checkbox"/> (5) Personal e-mail addresses <input type="checkbox"/> (6) Personal home addresses		
<input type="checkbox"/> (7) Passwords <input type="checkbox"/> (8) Financial Information* <input checked="" type="checkbox"/> (9) Other (Specify): Scheduled retirement dates.		
*If Financial Information was selected, provide additional detail: <input type="checkbox"/> (a) Personal financial information <input type="checkbox"/> (b) Government credit card If yes, was issuing bank notified? <input type="checkbox"/> (c) Other (Specify):		
5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH		
a. PAPER DOCUMENTS/RECORDS (If selected, provide additional detail)		b. EQUIPMENT (If selected, provide additional detail)
<input type="checkbox"/> (1) Paper documents faxed <input type="checkbox"/> (2) Paper documents/records mailed <input type="checkbox"/> (3) Paper documents/records disposed of improperly <input type="checkbox"/> (4) Unauthorized disclosure of paper documents/records <input type="checkbox"/> (5) Other (Specify):		<input type="checkbox"/> (1) Location of equipment <input type="checkbox"/> (2) Equipment disposed of improperly <input type="checkbox"/> (3) Equipment owner <input type="checkbox"/> (4) Government equipment Data At Rest (DAR) encrypted <input type="checkbox"/> (5) Government equipment password or PKI/CAC protected <input type="checkbox"/> (6) Personal equipment password protected or commercially encrypted
c. IF EQUIPMENT, NUMBER OF ITEMS INVOLVED		
<input type="checkbox"/> (1) Laptop/Tablet <input type="checkbox"/> (2) Cell phone <input type="checkbox"/> (3) Personal Digital Assistant		<input type="checkbox"/> (4) MP3 player <input type="checkbox"/> (5) Printer/Copier/Fax/Scanner <input type="checkbox"/> (6) Desktop computer
<input type="checkbox"/> (7) Flash drive/USB stick/other removable media <input type="checkbox"/> (8) External hard drive <input type="checkbox"/> (9) Other		(If Other, Specify):
<input checked="" type="checkbox"/> d. EMAIL (If selected, provide additional detail)		<input checked="" type="checkbox"/> e. INFO DISSEMINATION (If selected, provide additional detail)
<input type="checkbox"/> (1) Email encrypted <input type="checkbox"/> (2) Email was sent to commercial account (i.e., .com or .net) <input type="checkbox"/> (3) Email was sent to other Federal agency <input type="checkbox"/> (4) Email recipients had a need to know		<input type="checkbox"/> (1) Information was posted to the Internet <input type="checkbox"/> (2) Information was posted to an intranet (e.g., SharePoint or Portal) <input type="checkbox"/> (3) Information was accessible to others without need-to-know on a share drive <input type="checkbox"/> (4) Information was disclosed verbally <input type="checkbox"/> (5) Recipients had a need to know
<input type="checkbox"/> f. OTHER (Specify):		
6.a. TYPE OF INQUIRY (If applicable) (Click to select) (If Other, specify) Internal		b. IMPACT DETERMINATION (for Component Privacy Official or designee use only) (X one) <input type="checkbox"/> Low <input type="checkbox"/> Medium <input checked="" type="checkbox"/> High
c. ADDITIONAL NOTES (Up to 150 words, bullet format acceptable) NOTE: Do NOT include PII or Classified Information. Five factors should be weighed to assess the likely risk of harm: • Nature of the data elements breached - SSN, DOB, and retirement • Number of individuals affected - 12 • Likelihood the information is accessible and usable - records were immediately removed from AKO upon notification date/time stamp shown record was published for four days, personnel who received the e-mail were asked to delete it and provide additional sources they may have forwarded it to. • Likelihood the breach may lead to harm - low • Ability of the Department to mitigate the risk of harm - high CASCOM G-6 POC i.am.reporting.civ@mail.mil (804) 765-XXXX		

DD FORM 2959 (BACK), FEB 2013

Figure D-1. Sample DD Form 2959, cont.



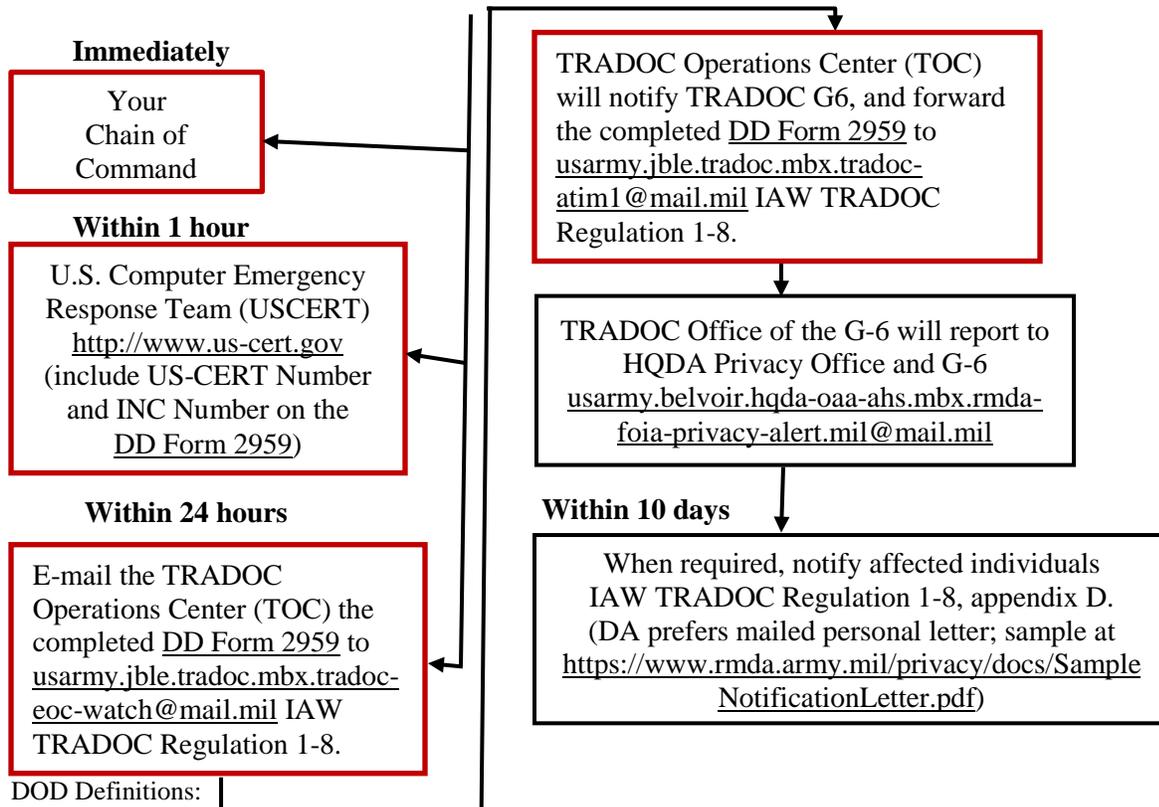
Reporting Loss or Suspected Loss/Breach of PII Flow Chart



TRADOC Organization XXX

Military and civilian personnel will report possible and confirmed breach to:

- 1) Their organization's information assurance security officer/security officer _____ via e-mail: _____ or DSN XXX-XXXX or commercial (XXX) XXX-XXXX.
- 2) The following organizations/personnel within the time limits noted below:



DOD Definitions:

- **Personal information definition:** Information about an individual that identifies, links, relates, or is unique to, or describes him or her, for example, a social security number; age; rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information.
- **PII definition:** Information which can be used to distinguish or trace an individual's identity (such as, their name, SSN, date and place of birth, mother's maiden name, biometric records including other personal information which is linked or linkable to a specific individual).
- **Lost, stolen, or compromised information:** Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected. Such incidents are known as breaches.
- **Record definition:** Any item, collection, or grouping of information, whatever the storage media (paper, electronic, etc.) about an individual that is maintained by a DOD component.
- **Review notification guidance** DOD and Army Guidance on PII Breach Notifications: <https://www.rmda.army.mil/privacy/RMDA-PO-Infractions.html> and <http://dpclo.defense.gov/Privacy/AbouttheOffice/PolicyandGuidance.aspx>.
- **Privacy Act compliance** and managerial training and videos <https://www.rmda.army.mil/privacy/RMDA-PO-Training.html>.

Figure D-2. Sample TRADOC center/activity Breach Report PII Flowchart

e. 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 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 to remind 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. See [Privacy Act compliance](#) and managerial training and videos, for remedial training.

D-5. Identity theft risk analysis

Commanders/directors will consider five factors when assessing the likelihood of risk of harm. See the U.S. Army Records Management and Declassification Agency [PII Breach: Risk Determination](#). 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.

(1) After evaluating each of the five factors, reassess the level of impact already assigned to the information using impact levels defined by National Institute of Standards and Technology (NIST). [Federal Information Processing Standards Publication 199](#) and NIST Special Publication [800-122](#) define three levels of potential impact on organizations or individuals.

(2) 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 must be indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years.

E-4. Test questions

- a. What is the correct format used for SIRs (SIR format in [AR 190-45](#))?
- b. Are initial telephonic/e-mail notifications of SIR incidents reported to the TOC immediately upon discovery or notification at the installation level?
- c. Are initial written SIRs sent to the TOC within 4 hours of initial discovery or notification at the installation level?
- d. Do initial SIRs contain all the relevant information (who, what, when, where, how, and why) available at the time?
- e. Are follow-up reports forwarded to the TOC within 2 hours of the request for follow-up information?
- f. Are SIRs digitally signed and encrypted from the originator through all the intermediate approval levels to the TOC?
- g. Are SARs used in accordance with 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 Senior Command's 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, Current Operations (G-33), DCS, G-3/5/7 (ATTG-OPA), 950 Jefferson Avenue, Fort Eustis, VA 23604.

Appendix F

Command, control, communications, and computers (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. POC for Appendix F is Mr. Larry Franklin, larry.franklin1.civ@mail.mil, Phone (757) 501-6555.

F-2. Unplanned C4 degradation within Installation Operations Centers (IOCs) and/or TRADOC activities

a. IOC:

(1) Notify TOC by e-mail to usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.mil to report any unplanned, significant 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 usarmy.jble.tradoc.mbx.tradoc-eoc-watch@mail.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 usarmy.jble.tradoc.list.tradoc-g-6@mail.mil.

(2) Place information in the Daily Event Summary.

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 degradation of C4 capabilities (paragraph F-1).

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

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

Glossary

Section I

Abbreviations

AR	Army regulation
C4	command, control, communications, and computers
CAT	category
CCIR	Commander's Critical Information Requirement
CG	commanding general
DA	Department of the Army
DA Pam	DA Pamphlet
DCS	deputy chief of staff
DD Form	Department of Defense Form

DOD	Department of Defense
DSAID	Defense Sexual Assault Incident Database
DSN	Defense Switched Network
EOC	emergency operations center
ERP	Electronic Reporting Portal
FOUO	For Official Use Only
HIPAA	Health Insurance Portability and Accountability Act
HQ	headquarters
IOC	installation operations center
NIPRNET	non-secure internet protocol router network
NIST	National Institute of Standards and Technology
PII	personally identifiable information
ROTC	Reserve Officer Training Corps
SAR	Suspicious Activity Report
SIPRNET	secure internet protocol router network
SIR	serious incident report
SC	senior commander
SSN	social security number
TOC	TRADOC Operations Center
TRADOC	U.S. Army Training and Doctrine Command
U.S.	United States
USACIDC	U.S. Army Criminal Investigation Division Command
USAREC	U.S. Army Recruiting Command
US-CERT	U.S. 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.

TRADOC Regulation 1-8

TRADOC Soldiers

Includes all Soldiers assigned, attached, operational control and contracted ROTC cadets.

Officer Initial Entry Training

Includes Basic Officer Leaders Course-A and Basic Officer Leaders Course-B, Warrant Officer Candidate School and Warrant Officer Basic Course. Basic Officer Leaders Course-A includes ROTC (reports to Cadet Command), USMA (direct reporting unit), and Officer Candidate School.