United States Army Cadet Command
SOP 23-11

Operations

U.S. Army Cadet Command Incident Reporting

Headquarters
United States Army Cadet Command
Ft. Knox, KY
27 January 2025

UNCLASSIFIED

SUMMARY of CHANGES

USACC Standard Operating Procedure
U.S. Army Cadet Command Incident Reporting

- This SOP replaces USACC SOP 23-11, dated 5 March 2024.
- Updated USACC CCIR Matrix.
- Updated verbiage throughout SOP.
- Updated Serious Incident Report Format.
- Updated Suspicious Activity Report Format.
- Updated responsibilities section.

Department of the Army
Headquarters, United States Army Cadet Command
1st Cavalry Regiment Road
Fort Knox, Kentucky 40121-5123

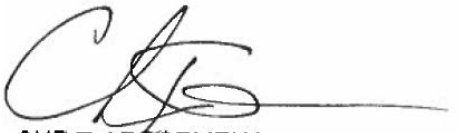
Effective 27 January 2025

Operations

U.S. Army Cadet Command Incident Reporting

FOR THE COMMANDER:

OFFICIAL:



CHE T. AROSEMENA
COL, GS
Chief of Staff

MAURICE BARNETT
Brigadier General, U.S. Army
Commanding

History: This printing publishes USACC SOP 23-11 Incident Reporting. This publication replaces current U.S. Army Cadet Command (USACC) SOP 23-11, 5 March 2024.

Summary: This SOP prescribes the operational reporting of significant incidents to Headquarters (HQ), USACC.

Applicability: This SOP applies to all elements of USACC, to include HQ USACC, subordinate commands, activities, and units, including those elements not on an installation. This SOP also applies to non-organic elements while in a direct supporting role of Cadet Summer Training (CST).

Proponent and exception authority: The proponent of this SOP is the USACC Chief of Staff. The proponent has the authority to approve exceptions or waivers to this SOP 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 SOP 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.

Army management control process. This SOP 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 SOP is prohibited without prior approval from the Deputy Chief of Staff, G-3, Chief, G-3 Operations Division (ATCC-TOC), 1st Cavalry Regiment Road, Fort Knox, KY 40121.

Suggested improvements. Users are invited to send comments and suggested improvements on Department of the Army Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Deputy Chief of Staff, G-3, Chief Operation Division (ATCC-TOC), 1st Cavalry Regiment Road, Fort Knox, KY 40121.

Distribution. Distribution of this SOP is intended for HQ USACC and its subordinate units. Distribution is in electronic format only.

Contents (Listed by paragraph and page number)

Chapter 1 1

1-1. Purpose 1

1-2. References 1

1-3. Explanation of Abbreviations 1

1-4. Responsibilities 1

Chapter 2 3

2-1. Policy 3

2-2. Reportable events and incidents 3

2-3. Report Type 4

2-4. Additional Guidance 7

Chapter 3 9

3-1. Time requirements 9

3-2. Required Information 11

3-3. Handling of reports 11

3-4. Parallel report(s) 11

3-5. Request for Information 11

Appendix A – References 13
Appendix B – CCIR Matrices (USAREC & USACC) 15
Appendix C – SIR Formats 20
Appendix D – DR Format 25
Appendix E – SAR Format 27
Appendix F – PII Breach Report 29
Appendix G – Management Control Checklist 37
Appendix H – RFI Format 39
Appendix I – Glossary 40

Chapter 1
Introduction

1-1. Purpose

This SOP establishes policies and procedures for the reporting of significant incidents involving USACC facilities, activities, and personnel. The primary purpose of this process is to provide a means to inform USACC and U.S. Army Recruiting Command (USAREC) senior leadership of incidents which impact USACC elements. The secondary purpose is to provide HQ USACC 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. This SOP combines Incident Reports (IR), PII/Cyber Incidents, Suspicious Activity Reports (SAR), Disaster Reporting (DR), Force Protection Condition Change reporting and Commanders Critical Information Requirements (CCIR), Friendly Forces Information Requirements (FFIR) and Priority Information Requirements (PIR) into one SOP. Reportable incidents listed in this SOP are not all inclusive. **Commanders should use discretion in reporting incidents that are not specifically listed in this SOP**.

1-2. References

The primary sources for reporting requirements are the USACC Commander's Critical Information Requirements, USAREC Information Requirements, Law Enforcement Reporting (Army Regulation 190-45), ARs, DA Pams, and DA Forms are available at http://www.armypubs.army.mil/. A list of publications can be found in Appendix A.

1-3. Explanation of Abbreviations

Common abbreviations and terms used in this SOP are contained in the Glossary.

1-4. Responsibilities

USACC HQs, USACC subordinate commanders, USACC activity, unit, and Headquarters and Headquarters Detachment (HHD) personnel will ensure that the policies and procedures of this SOP are implemented in their organizations.

a. Commanding General (CG), USACC is responsible for reporting the events and incidents defined in the USAREC CCIR Matrix, as well as any other matter that the CG determines to be of concern to the CG, USAREC.

b. USACC HQs, staff directorates, subordinate commanders, activities, units, and HHD personnel are responsible for reporting the events and incidents defined throughout this SOP, as well as any other matter that commanders determine to be of concern to the CG, USACC.

c. Brigade Commanders will appoint a Primary and Alternate Incident Manager. Incident managers will ensure reports are properly formatted, accurate, and include all required information.

d. USACC HQs staff will submit reports through the HHD Commander. Subordinate units report through their respective Brigades. CST personnel report through the CST TOC.

e. Deputy Chief of Staff (DCS), G-3, Chief Operations Division (G-3), or an Operations Division (G-3) representative is responsible for notifying the USACC Command Group and USACC staff of SIRs.

f. DCS, G-3, Operations Division Security Specialist or a G-3 designated representative will analyze each SAR and ensure U.S. Army Criminal Investigation Division (USACID) enters the incident into eGuardian if it meets the eGuardian criteria. DCS, G-3, Operations Division Security Specialist or designated representative is responsible for collecting, analyzing, and referring all SIRs and SARs to the Chief, Operations Division (G-3), USACC leadership, and to appropriate HQ and staff sections, adjacent, and higher commands as appropriate. The G-3 Security Specialist will receive reports, request follow-ups, and report incidents to the USACC leadership and to USAREC staff via the approved procedures and maintain a database of reported incidents for trend analysis.

g. The DCS, G-6 is responsible for updating PII guidance, as necessary.

h. Brigades will submit JROTC related incidents through the Brigade Incident Manager to the Operations Division (G-3). JROTC reports that include any form of JROTC Instructor misconduct, must list the date that the instructor signed the DD Form 3200 (JROTC INSTRUCTOR PROHIBITED ACTIVITIES ACKNOWLEDGEMENT).

Chapter 2
Reporting Policy

2-1. Policy

a. All reports must be submitted using USACC incident report guidance, completed correctly and in the proper format. Incomplete reports will be returned to the Brigade Incident Manager for correction and resubmission. Failure to submit reports IAW established guidelines could result in late reports that require a commander's endorsement for lateness. As the information concerned is developed, subordinate commands will submit follow-up reports, corrections to reports, and final reports in accordance with (IAW) Chapter 3 Reporting Procedures. Reports are sent to the USACC SIR Points of Contact (POC(s)) via encrypted email to; USARMY Ft Knox USACC List SIR usarmy.knox.usacc.list.sir@army.mil.

b. Report incidents to HQ, USACC, as listed in Appendix B USACC CCIR Matrix. The lists are not all inclusive. Commanders and Professors of Military Science (PMS) should report any incident that might concern the CG, USACC as a serious incident, regardless of whether specifically listed. In determining whether an event/incident is of concern to CG, USACC, 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 an SIR.

c. Reporting procedures outlined in this SOP support the reporting procedures outlined in AR 190-45 (Law Enforcement Reporting) or the submission of other reports (for example, SHARP Related Incidents, PII breach, SAR, or mishap reports submitted through separate reporting channels). Parallel reports are often required due to specific incident types.

d. Direct coordination between organizations, offices, agencies, or activities within USACC is authorized and encouraged. In addition, all USACC subordinate headquarters will coordinate directly with local supporting law enforcement/campus security agencies, Provost Marshal Office (PMO), Criminal Investigation Division (CID) or Joint Terrorism Task Forces (JTTF) on matters of force protection or criminal activity. Commanders and representatives must realize the reporting of incidents or coordination with outside activities will generate reports within that agency. It is therefore mandatory that any outside coordination is reported to the next higher headquarters.

e. Simultaneous with official reporting through operational channels, CG, USACC, or their designated representative, will provide the CG and DCG, USAREC an email with the 7 "Ws" amplification of serious incidents. This "Green Tab" parallel information is in addition to the official operations reporting requirement.

2-2. Reportable events and incidents

USACC 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. USAREC CCIRs as published in USAREC Operation Orders and Fragmentary Orders.

c. AR 190-45 and SIRs per Chapters 8 & 9, Category (CAT) I & II reportable incidents.

d. USACC CCIRs as published in USACC Operations Orders and Fragmentary Orders. Current USACC CCIR Matrix is located at Appendix B.

2-3. Report Type

Each type of report is described below. Specific report formats and other written requirements are contained in subsequent areas of this SOP.

All report types below are reported as an Initial, Follow-Up, or Final report.

a. **Serious Incident Report (SIR):** These reports include all CCIR and additional incidents.

*Note: Report format located at Appendix C.

(1) CCIR: Incidents which are of great concern to the commander, includes Friendly Force Information Requirements (FFIR) and Priority Intelligence Requirements (PIR). These incidents are contained in the CCIR Matrix located in Appendix B.

(2) USACC Other Reporting Requirements**:** This category includes incidents that do not meet CCIR criteria, but based on their risk, severity and unit impact are reportable IAW applicable regulations and higher headquarters guidance.

b. **Disaster Report (Natural/Manmade):** Disasters require the submission of disaster incident reports when the result of a disaster causes displacement of personnel and/or National Guard and Army Reserve activations of Cadre and Cadets. In addition, disaster reports are required when the operational capabilities of a unit are affected so as to limit the unit's capabilities to support the mission. The Disaster Report is submitted to the USACC Protection Division as an unencrypted email. Report format located at Appendix D.

(1) All disasters, natural and technological – manmade, will be reported as a Disaster Report that affects operations and displacement of Soldiers, family members, or the civilian workforce.

(2) Initial disaster reporting requirements:

- Accountability of USACC personnel including family members and cadets affected.

- Identify the number of personnel displaced by the disaster.

- Name(s) of all affected USACC facilities and any initial actions taken by the unit.

- Any higher headquarters assistance requested.

(3) Follow up reports are due every 24 hours at 1300 hours (EST) to the USACC Operations Center. Follow up reports must include all information in the report format. Reports will not be closed until normal operations resume and any activated personnel return to regular duty.

(4) Place Request for Assistance (RFA) in bold in the block and provide specific needs that are above the capabilities of the brigade, program, or university.

(5) Commanders should focus on taking care of personnel and resumption of mission operations as soon as possible.

USACC Disaster Reporting	
Natural	**Technological - Manmade**
Drought	Power Failure
Earthquake	Terrorism
Floods	Transportation Accident
Wildfire	Civil Disorder
Tornado	Dam Failure
Hurricane	Fuel Shortages
Windstorm	Hazardous Materials Incident
	Mass Cyber Attack

c. **Suspicious Activity Report:** The intent of suspicious activity reporting is to ensure that USACC leadership have a clear picture of the scale of these phenomena by capturing the information. SARs will be reported in the same manner as SIRs. The raw data information collected and reported on the SAR allows the intelligence community to analyze trends and provide actionable intelligence for commanders to use in decision making.

Reportable suspicious incidents include:

1. Defined Criminal Activity and Potential Terrorism Nexus Activity

    a. Breach/Attempted Intrusion. Unauthorized person attempting to enter or actually entering a restricted area, or nonpublic area. Impersonation of authorized personnel.

    b. Misrepresentation. Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.

c. Theft/Loss/Diversion. Stealing or diverting something associated with a facility/infrastructure or secured protected sites such as uniforms, IDs, etc.

d. Sabotage/Tampering/Vandalism. Damaging, manipulating, defacing, or destroying part of a secure site.

e. Cyberattack. Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.

f. Expressed or Implied Threat. Communicating a threat to commit a crime that will result in death or bodily injury to another or to damage or compromise a secure site.

g. Aviation Activity. Learning to operate, operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism/criminality in a reasonable person. This category also includes unmanned aerial systems (UAS) and drone use that may be construed as suspicious (photography, criminal acts, etc.).

2. Potential Criminal or Non-Criminal Activities Requiring Additional Information

a. Eliciting Information. Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about an event or particular facets of a facility's purpose, operations, security procedures, etc.

b. Testing or Proving of Security. Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities.

c. Recruiting/Financing. Providing direct financial support to criminals and/or criminal/terror organizations; compiling personnel data, banking data, travel data, or contacts to build operational teams.

d. Surveillance/Photography. An interest in or taking pictures/videos of personnel, facilities, security features, or infrastructure in an unusual or covert manner. Drones may also be used in this capacity.

e. Material Acquisition/Storage. Acquisition and/or storage of unusual quantities of precursor materials (fuel, chemicals, toxic materials, timers, cell phones, or other triggering devices).

f. Acquisition of Expertise. Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities.

g. Weapon Collection/Discovery. Collection or discovery of unusual amounts or types of weapons, explosives, chemicals, or shows evidence of, detonations or other residue, wounds, or chemical burns.

h. Sector Specific Incident. Actions associated with a characteristic of unique concern to specific sectors (e.g., the education, public health, government, etc.), with regard to their personnel, facilities, systems, or functions.

(13) Report format located at Appendix E.

d. **PII Breach Report:** PII breach report is initiated when there is actual or suspected compromise of PII. The breach will be reported via the SIR process. PII breach actions and instructions are located at Appendix F.

e. **Sexual Harassment and Assault Reporting:** The intent of the SHARP report (located in Appendix C) is to provide the required information IAW AR 600-20 (Army Command Policy). All known personnel information (victim(s) and subject(s)) will be reported to the USACC SIR team. USACC SIR team will redact the necessary information before submitting to the staff and USAREC. When reporting sexual harassments only include the type of sexual harassment (quid pro quo and/or hostile environment, wrongful broadcast of distribution of intimate visual images, indecent viewing, recording, or broadcasting), DO NOT include specific details of the harassment. When reporting sexual assault include the type of assault and what crime is being investigated (rape, sexual assault, aggravated sexual assault, abusive sexual contact, or sodomy), DO NOT include specific details of the assault (IAW AR 600-20, App. J-2). Brigades will ensure their supporting SARC/VA review all reports of sexual harassment and/or assault prior to submitting to HQs, USACC.

2-4. Additional Guidance

a. **Suicide Attempts:** The Commander, Command Sergeant Major or Command representative as soon as medically permissible will conduct a face-to-face discussion with each Soldier who has attempted suicide. The intent is to develop a better understanding of the Soldier's situation and environment and to identify any potential action(s) that may prevent suicidality. The end state of the discussion should reveal responses to five key questions (**within 96 hours from initial report**):

(1) All that we know now?
(2) What we didn't know?
(3) What we wish we had done but did not do?
(4) What lessons were learned?
(5) Was the Soldier part of a cohesive team – unit, battle buddy, family connections?

b. **Suicides/Suspected Suicides:** Commanders at all levels will develop and submit a DA Form 7747 (Commander's Suspected Suicide Event Report) for every suicide or equivocal death which is being investigated as a possible suicide. Active duty units are

required to submit Section 1 of the DA 7747 within 24 hours to usarmy.pentagon.hqda-dcs-g-1.mbx.csser@army.mil within 24 hours of the incident, IAW AR 190-45, para 9-2b. Section II of the DA From 7747 is required within five days of the incident. The report is completed with the submission of Section III within 60 days of the incident. Within 96 hours of initial report provide answers to the five key questions, listed in paragraph 2-4a and provide to the USACC G33 SIR team.

c. **GSA Incidents:** Reports on incidents related to GSA vehicles including vehicle accidents, theft, vandalism and sabotage will include the year, make, model, color, tag number and VIN of the impacted GSA(s). Acts of vandalism and sabotage may require photos of the damage.

Chapter 3
Reporting Procedures

3-1. Time requirements

a. **Immediate**: For incidents on the USACC CCIR list; the Brigade Commander or representative will notify a member of the command group (CG, DCG, Chief of Staff or Deputy Chief of Staff) immediately upon identification of a CCIR related incident. The Brigade will first attempt to contact the CG. If the CG does not acknowledge receipt within 15 minutes, then the Brigade will contact, in order, the DCG, CoS, and the ACoS until acknowledged.

b. **Two Hours**:

(1) Brigade Commander or representative will follow up the CCIR telephonic notification with a 7W's message (who, what, when, where, why, actions taken, assistance required) within two hours of the incident identification. Recipients of the 7W's are; CG, DCG, CoS, ACoS, DCS G3, G3 SIR POC list (usarmy.knox.usacc.list.sir@army.mil). CG, USACC may require additional actions or information.

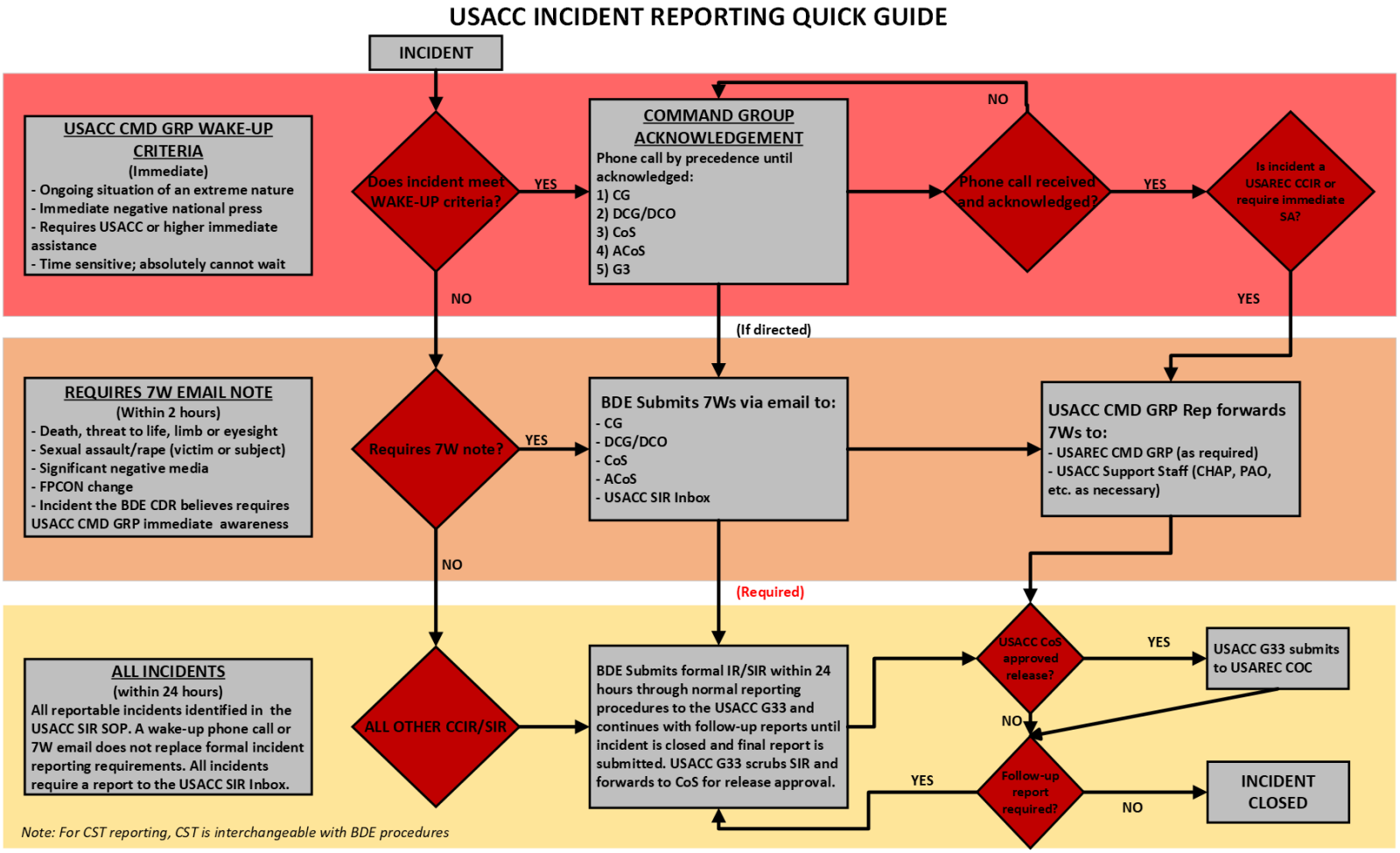
c. **24 – 48 hours**: Written initial reports are due in SIR format, located in Appendix C, to the next higher headquarters. Incident managers will also include the text of the SIR in the body of the email to reduce timeliness when document encryption issues occur.

(1) Initial Reports are due within 24-48 hrs. or the next duty day.

(2) Follow-Up Reports are required as information changes.

(3) Final Reports are submitted once administrative actions and investigations are concluded or a final disposition is reached.

(4) All Open Reports will be reviewed by HQs, USACC. Submitting units will review open reports monthly to ensure timely updates/closure. The Operations Division (G-3) will provide a monthly open report roll-up to the Brigade Incident Managers.



USACC SIR Inbox: usarmy.knox.usacc.list.sir@army.mil

Figure 1. USACC Incident Reporting Quick Guide

3-2. Required Information

a. All pertinent information will be entered onto the proper report format. The report formats are located in the appendices. Reports will include all available, relevant facts and information. This includes, but is not limited to: names, addresses, next of kin and any other information pertinent to the clear understanding of the incident being reported. All items on the required format will be completed with information available at the time of submission.

b. Brigades will assign each report a tracking number and submit all reports via email to the USACC SIR POCs. The numbering system used will be the following:

(1) Initial reports: Brigade/fiscal year/sequence number of initial report, incident type (e.g., the first SIR from 1st Brigade in FY 2025 would be numbered (1st BDE-25-001, Death-INITIAL)).

(2) Follow-up reports: Assign letters to denote follow-up reports and replace "INITIAL" with "FOLLOW-UP" (e.g., 1st BDE-20-001A, Death-FOLLOW-UP). New information provided on follow-up reports will no longer be in all CAPS.

(3) Final reports: When the SIR issue is resolved, the final report number will include "FINAL" (e.g., 1st BDE 20-001B, Death-FINAL). Final information will be annotated in line 12 of original SIR and conform to requirements outlined in sub-paragraphs (1) and (2) above.

3-3. Handling of reports

a. Due to the potentially sensitive nature of SIRs all e-mails and reports will be marked at a minimum of Controlled Unclassified Information (CUI). Data sent 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. POCs will only transmit personal health information in SIRs as it relates to the SIR incident. POCs 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. Parallel report(s)

Incidents sometimes require cross reporting lines, coordination, or reports to other agencies. The coordination will generate reports from the agency involved. The reporting unit is required to notify their next Higher Headquarters (HHQ) of any outside coordination or reports for awareness and assistance as necessary.

3-5. Request for Information

Additional information may be required by a higher headquarters or other agency to execute actions that are a result of the incident (e.g., disenrollment from a program, revocation of security clearances, etc.). In order to preserve the privacy of all parties,

requests for information specific to individuals involved in an incident will be processed with the same protections as the initial report. All Requests for Information (RFIs) are sent via encrypted email.

a. Request will be forwarded to the USACC SIR POC.

(1) Each request will clearly state the information required and a suspense date/time group (DTG) will be provided in order to facilitate expedience.

(2) USACC SIR POC will forward the request to the respective brigade/organization POC.

(3) Brigade/organization POC will gather and provide the requested information to the USACC SIR POC.

(4) USACC SIR POC will forward the information to the requesting agency to close out the request.

(5) RFI format is located at appendix H

Appendix A – References

References

Section I
Required Publications

ARs, DA Pamphlets, and DA forms are available at www.armypubs.army.mil. USAREC publications and forms are available at https://adminpubs.USAREC.army.mil. DoD publications and forms are available at https://www.esd.whs.mil/Directives/issuances/dodi/.

DoDM 5400.11-R, DoD Privacy Program

AR 25-2, Army Cybersecurity

AR 145-1, SROTC Program, Organization, Administration, and Training

AR 190-45, Law Enforcement Reporting

AR 190-59, Chemical Agent Security Program

AR 200-1, Environmental Protection and Enhancement

AR 360-1, The Army Public Affairs Program

AR 380-13, Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

AR 385-10, Army Safety Program

AR 420-1, Army Facilities Management

DA Pamphlet 600-24, Health Promotion, Risk Reduction and Suicide Prevention

Section II
Related Publications

AR 11-2, Managers Internal Control Program

AR 40-5, Army Public Health Program

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DA Form 2028, Recommended Changes to Publications and Blank Forms

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

USACC COMMANDERS CRITICAL INFORMATION REQUIREMENTS (CCIR) MATRIX

As of: December 12, 2024

	INCIDENT/EVENT	Category	Notify USACC CMD GRP[4]	Report to USAREC	Report to HQDA	USAREC CCIR	Regulatory/Policy Guidance
	USACC CCIRs (FFIR - PIR)						
FFIR 1	Death of any USACC military personnel, civilian employee (DAC or Contractor), JROTC instructor, contracted SROTC Cadets, immediate family members (spouse, child or legal dependent), SROTC non-contracted/JROTC Cadets (during official ROTC activities).	DEATH	Yes	Yes	Yes	2	DA Reportable
FFIR 2	Serious injury or illness involving threat to life, limb or eye sight of any USACC military personnel, civilian employee (DAC or Contractor), JROTC Instructor, contracted SROTC Cadets, immediate family members (spouse, child or legal dependent), SROTC non-contracted/JROTC Cadets (during official ROTC activities).	SERIOUS INJURY/ILLNESS	Yes	Yes	Yes	20/29/45	USAREC Reportable
FFIR 3	Changes to FPCON or changes to other alert and security status levels or additions to any FPCON measure directed either by DA, HHQ, unit commander or prompted by a threat reported in the vicinity of any USACC facility or asset.	ATFP	Yes	Yes	Yes	24/38	DA Reportable
FFIR 4	Missing, Absent-Unknown, Absent Without Leave, and Duty Status-Whereabouts Unknown of any USACC military personnel, civilian employee (DAC or Contractor), JROTC instructor, contracted SROTC Cadets, immediate family members (spouse, child or legal dependent), SROTC non-contracted/JROTC Cadets (during official ROTC activities).	MISSING PERSON	Yes	Yes	Yes	USACC	AR 190-45
FFIR 5	Reports or allegations of SHARP related incidents to include, but not limited to sexual assault (including rape), sexual harrassment, abusive sexual contact by or against any USACC military personnel, civilian employee (DAC or contractor), JROTC Instructor, SROTC Cadets (contracted or non-contracted) and JROTC Cadets (during USACC sponsored activities).	MISCONDUCT	Yes	Yes	Yes	4	DA Reportable
FFIR 6	USACC Military, civilian employee (DAC or Contractor), SROTC Cadet, JROTC Instructor or JROTC Cadet exhibiting indicators of actual/potential violence or extremist/racist behavior.	MISCONDUCT	Yes	Yes	Yes	40	AR 190-45
FFIR 7	Any planned or unscheduled Distinguished Visitors (DV)[1] to USACC or subordinate organizations.	DV/VIP	Yes	Yes	Yes	32	DA/USAREC Reportable
FFIR 8	Any allegation or incident of misconduct against or by USACC Military, Civilian Employee (DAC or Contractor), contracted SROTC Cadet, JROTC Instructor, or SROTC non-contract/JROTC Cadets (during USACC sponsored activities).	MISCONDUCT	Yes	Yes	Yes	5/6/46	OSD/DA/USAREC Reportable
FFIR 9	Any incident of concern based on the nature, gravity, potential for adverse publicity, or potential consequences of the incident.	MEDIA/OTHER	Yes	Yes	Yes	1/11	AR 190-45
FFIR 10	Any crime committed by or against any USACC Military, Civilian Employee (DAC or Contractor), contracted SROTC Cadet, JROTC Instructor or SROTC non-contract/JROTC Cadets (during USACC sponsored activities).	MISCONDUCT	Yes	Yes	Yes	3	USAREC Reportable
PIR 11	Imminent threat to Army Senior Leaders.	ATFP	Yes	Yes	Yes	12	DA Reportable
PIR 12	CBRN event whether confirmed or suspected, to include the misuse of riot control agents.	ATFP	Yes	Yes	Yes	13	DA Reportable
PIR 13	Manmade or natural disasters impacting USACC personnel on or off installations across CONUS and overseas.	ATFP	Yes	Yes	Yes	24	DA Reportable
PIR 14	Foreign collection activities (surveillance, elicitation, solicitation, etc.) targeted against USACC activities, schools, personnel, and interests.	ATFP	Yes	Yes	Yes	8	DA Reportable
PIR 15	Any threat, attack or incident at a government or non-government facility or event directed at or affecting USACC personnel or equities.	ATFP	Yes	Yes	Yes	7/14/16/47	DA Reportable
PIR 16	Theft, suspected/attempted theft, loss, targeting, tracking or threat against AA&E (including arms rooms) or chemical agents.	ATFP	Yes	Yes	Yes	30	AR 190-45
PIR 17	Any indications or impacts of ongoing adversary cyber warfare efforts, cyber attacks, incidents or intrusions on USACC information systems CONUS/OCONUS.	CYBER	Yes	Yes	Yes	9	DA Reportable
PIR 18	Suspicious Activity[3] (includes theft of government property, vandalism of USACC facilities, GSAs, suspicious packages, etc.).	SAR	No	No	No	USACC	AR 190-45

USACC Other Reporting Requirements- Reportable SIRs IAW AR 190-45, AR 385-10, AR 25-2 and other Applicable Regulation							
ORR 19	Command, Control, Communications, and Computers (C4) outages. Activities will report planned and unplanned degradations lasting more than two hours or degradation that results in significant negative impact on the ability of senior leaders to exercise command and control. (AT ECHELON)	ATFP	No	Yes	No	36	USAREC Reportable
ORR 20	Any incident involving spillage of classified information.[6]	ATFP	Yes	Yes	Yes	10	USAREC Reportable
ORR 21	Major installation or campus utilities interruptions that impact operations and training. (AT ECHELON)	ATFP	No	No	No	USACC	AR 190-45
ORR 22	Hospitalization for a Mental Health (MH) condition, court order to consult with MH professional, diagnosis by an MH professional with a psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder or antisocial personality disorder.	BEHAVIORAL HEALTH	Yes	Yes	Yes	22/41	DA Reportable
ORR 23	Suicide attempt, ideations or self-harm (all overt acts of self-destructive behavior that do not result in death) committed by any USACC military personnel, civilian employee (DAC or Contractor), JROTC Instructor, contracted SROTC Cadets, immediate family members (spouse, child or legal dependent), SROTC non-contracted/JROTC Cadets (during official ROTC activities).	SELF-HARM	No	No	No	39	AR 190-45
ORR 24	Communicable illnesses/disease, such as influenza (all strains), hepatitis, COVID-19 and West Nile Virus that exceed the expected baseline (established by medical professionals) for those illnesses and unusual illnesses of any USACC Military, Civilian Employee (DAC or Contractor), SROTC Cadet or JROTC Instructor.	DISEASE/ILLNESS	No	No	No	37	USAREC Reportable
ORR 25	Suspected[2] or confirmed environmental injuries (such as heat stroke, rhabdomyolysis, carbon monoxide poisoning, hypothermia, frostbite and heat exhaustions) of any military personnel, civilian employee (DAC or Contractor), JROTC Instructor, contracted SROTC Cadets, SROTC non-contracted/JROTC Cadets (during official ROTC activities) assigned to USACC.	ENVIRONMENTAL INJURY/ILLNESS	No	No	No	42	AR 190-45
ORR 26	Any PII breach or compromise.	MISCONDUCT	No	No	No	43	AR 385-10
ORR 27	Suspension or relief for cause (personnel in a position of authority).	MISCONDUCT	Yes	Yes	No	21	AR 25-2
ORR 28	Actual or alleged incidents of child abuse by Army personnel.	MISCONDUCT	Yes	Yes	Yes	31	AR 190-45
ORR 29	Wrongful use, possession, manufacture or distribution of a controlled substance, ALL positive urinalysis, including narcotics and drugs.	MISCONDUCT	No	No	No	USACC	AR 190-45
ORR 30	Injuries/illnesses incurred during training, in the workplace or during Army operations that result in medical treatment greater than first aid[5], to include evacuation to a medical facility or hospitalization of any USACC military personnel, civilian employee (DAC or Contractor), JROTC Instructor, contracted SROTC Cadets, SROTC non-contracted/JROTC Cadets (during official ROTC activities).	INJURY/ILLNESS	No	Yes	Yes	27/28	AR 190-45
ORR 31	Accidental damage to GOV property, damage to civilian property or injury to civilians caused by GOV activities, including, but not limited to GSA accidents, roll-overs, accidental equipment damage, etc. (AT ECHELON)	MISHAP	No	No	No	USACC	AR 385-10/AR 190-45

NOTES

[1] Distinguished Visitors (DV) includes US/State Politicians, National Politicians, Presidential Appointees, US General Officers (LTG/GEN), Senior Executive Service (SES), any foreign general officer

[2] Follow-up reports must provide medical professional determination on whether injury is confirmed or not.

[3] Suspicious Activity Reports (SARs) - SARs are submitted via SIR and include defined criminal activity, potential nexus to terrorism, and other potential non-criminal activity that may have a nexus to crime or terrorism. These can include facility breaches, misrepresentation, theft/loss/diversion of government property, sabotage/vandalism, cyber attacks, threats, aviation activity, eliciting, testing security, surveillance, etc. For indivudal SAR categories and details refer to Chapter 2 of the USACC Reporting SOP.

[4] Refer to the USACC Incident Reporting Quick Guide for wake-up criteria and Command Group acknowledgement procedures.

[5] Medical treatment greater than first aid focuses on patient management and care beyond basic on-the-spot first aid. It does not include visits to medical professionals solely for observation, counseling, diagnostic procedures or first aid.

[6] 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 3-1in this document for more details).

[7] At Echelon: incidents in the catagory are reportable to the next higher command only. (Program-BDE, BDE-USACC HQs, USACC HQs-USAREC HQs)

USAREC Table 2-1 (Version 3.0) CCIR/SIR/UIR Reporting (Dated 4 SEP 24)

	Incident / Event	NOTIFY USAREC CG	REPORT TO HQDA AOC	USAREC ERP REPORTING TIME	DA CCIR#
USAREC CG CCIRs					
1	INCIDENT OF CONCERN TO HQDA, AFFECTING THE LIFE, HEALTH, OR SAFETY OD SOLDIERS, FAMILY MEMBERS, OR THE WORKFORCE; OR ANY OTHER INCIDENT THE CDR DETERMINES TO BE OF IMMEDIATE CONCERN TO HQDA BASED ON THE GRAVITY, NATURE, POTENTIAL FOR SIGNIFICANT ADVERSE PUBLICITY, OR CONSEQUENCES OF THE INCIDENT.	YES / PHONE	YES	0-4 HOURS	50
2	DEATH OF ANY SOLDIER, DEPENDENT, DA CIVILIAN, RESERVE OFFICER TRAINING CORPS (ROTC) CADET, OR CONTRACTOR ASSIGNED TO USAREC (ON OR OFF POST). IF THE MANNER OF DEATH IS UNKNOWN, THE INCIDENT WILL BE REPORTED AS "UNDETERMINED MANNER OF DEATH" AND THE MANNER OF DEATH WILL BE UPDATED BY (ADDENDUM) ADD-ON CCIR AS SOON AS DETERMINED. DUTY STATUS, NEXT OF KIN NOTIFICATION, ALCOHOL/DRUG INVOLVEMENT, DEPLOYMENT HISTORY WILL BE INCLUDED IN THE INITIAL CCIR. **NOTE:** FOUR CATEGORIES OF DEATH: NATURAL, ACCIDENTAL, SUICIDE, AND HOMICIDE.	YES / PHONE	YES	0-4 HOURS	19A/B/C
3	ALLEDGED SERIOUS CRIME (MURDER / ATTEMPTED MURDER, DOMESTIC VIOLENCE OR INTENTIONAL ASSAULTS CAUSING SERIOUS BODILY INJURY, OR LARCENY EXCEEDING $50K) COMMITTED BY OR AGAINST A USAREC SOLDIER, DEPENDENT, DA CIVILIAN, RESERVE OFFICER TRAINING CORPS (ROTC) CADET, OR CONTRACTOR.	YES / PHONE	YES	0-4 HOURS	N/A
4	ANY REPORT OF SEXUAL ASSAULT ALLEGATIONS (RAPE, SEXUAL ASSAULT, SEXUAL BATTERY, OR ABUSIVE SEXUAL CONTACT) COMMITTED BY OR AGAINST A USAREC SOLDIER, DEPENDENT, DA CIVILIAN, RESERVE OFFICER TRAINING CORPS (ROTC) CADET/ JROTC CADETS OR CONTRACTOR.	YES / PHONE	YES/JROTC	0-4 HOURS	N/A
5	ANY INSTANCE OF MISCONDUCT IN WHICH THE ALLEDGED SUBJECT OCCUPIES A POSITION OF SPECIAL TRUST OR AUTHORITY.	YES / E-MAIL	NO	0-4 HOURS	N/A
6	SEXUAL MISCONDUCT WITH SUBJECT OF RECRUITING EFFORTS / ROTC/JROTC CADETS (SRE DEFINED - ALL CONTACTS AND PROSPECTS INCLUDES ALL HIGH SCHOOL STUDENTS REGARDLESS OF QUALIFICATION FOR MILITARY SERVICE, APPLICANTS, OR MEMBERS OF THE FSTP OR SISTER SERVICE EQUIVALENT ARE PROHIBITED). **EXAMPLES OF MISCONDUCT: SEXUAL RELATIONSHIPS OR PHYSICAL CONTACT IS INVOLVED.**	YES / E-MAIL	YES/JROTC	0-4 HOURS	N/A
7	FOREIGN COLLECTION ACTIVITIES (SURVEILLANCE, ELICITATION, SOLICITATION, ETC.) TARGETING USAREC PERSONNEL, ASSETS, AND INTERESTS.	YES / PHONE	YES	0-4 HOURS	N/A
8	INDICATIONS AND IMPACTS OF ONGOING ADVERSARY CYBER WARFARE EFFORTS ON, ARMY, AND DOD INFORMATION SYSTEMS ACROSS CONUS AND OCONUS.	YES / PHONE	YES	0-4 HOURS	13A/B/C/D
9	ANY INCIDENT INVOLVING SPILLAGE OF CLASSIFIED INFORMATION THAT WOULD CAUSE GRAVE DAMAGE TO THE UNITED STATES, USAREC, OR SUBORDINATE COMMANDS.	YES / PHONE	NO	0-4 HOURS	N/A
10	ANY DIRECT SOLDIER INTERVENTION (NON-COMBAT) THAT RESULTS IN THE PRESERVATION OF LIFE (E.G., SUICIDE INTERVENTION, LIFESAVING ACTION, ETC.)	YES / E-MAIL	YES	0-4 HOURS	40

	Incident / Event	NOTIFY USAREC CG	REPORT TO HQDA AOC	USAREC ERP REPORTING TIME	DA CCIR#
HQDA CCIR REPORTING REQUIREMENTS					
11	IMMINENT THREAT TO SENIOR US ARMY LEADERS OR IMMEDIATE FAMILY MEMBERS (ANY PRESIDENTIAL APPOINTED DA CIVILIAN, ANY GO OR SES, SMA) (LIMDIS ONLY)	or immediate family members	YES	0-4 HOURS	1
12	ANY CBRN EVENT THAT POSES A POTENTIAL THREAT TO US FORCES OR CITIZENS (E.G., FACILITIES LEAK, INDISTRIAL ACCIDENT, RENDER SAFE ACTTION, DISCOVERY, OR USE OF CBRN WEAPONS AGAINST US, COALITION, OR US CITIZENS. (SIPR ONLY)	YES / PHONE	YES	0-4 HOURS	2
13	ANY BREACH, ATTACK, THREAT, OR INCIDENT ADVERSELY IMPACTING US ARMY FACILITIES, EQUITIES, OR STRUCTURES.	YES / PHONE	YES	0-4 HOURS	3A
14	ANY REPORT OF SUSPICIOUS PACKAGE(S) AT US ARMY INSTALLATIONS, FACILITIES, OR STRUCTURES REQUIRING EOD/CBRN SUPPORT.	YES / PHONE	YES	0-4 HOURS	3B
15	ANY THREAT, ATTACK, OR INCIDENT AT A NON GOVERNMENT FACILITY OR EVENT THAT AFFECTS US ARMY PERSONNEL OR EQUITIES.	YES / PHONE	YES	0-4 HOURS	3C
16	INDIVIDUAL ON THE KNOWN / SUSPECTED TERRORIST (KST) WATCH LIST ATTEMPTS TO GAIN ACCESS TO ANY ARMY INSTALLATION, FACILITY, OR EQUITY. (SIPR ONLY). ADDITIONAL REPORTING REQUIRED ICW WITH AR 190-45 CHAPTER 8.	YES / PHONE	YES	0-4 HOURS	3D
17	US ARMY CLASS A AVIATION ACCIDENT / INCIDENT WITH LOSS OF LIFE.	YES / PHONE	YES	0-4 HOURS	6A
18	US ARMY CLASSES A OR B AVIATION ACCIDENT / INCIDENT WITHOUT LOSS OF LIFE.	YES / E-MAIL	YES	0-4 HOURS	6B
19	VERY SERIOUS INJURY OR DEATH OF A SENIOR US ARMY LEADER (ANY PRESIDENTIAL APPOINTED CIVILIAN, ANY GO OR SES, SMA). (LIMDIS ONLY)	YES / PHONE	YES	0-4 HOURS	7A
20	SUSPENSION OR RELIEF OF ANY LTC OR ABOVE IN A COMMAND POSITION INCLUDING ALL USACC PMS POSITIONS. (LIMDIS ONLY)	YES / PHONE	YES	0-4 HOURS	7B
21	ANY US ARMY PERSONNEL REPORTED AS MISSING WHEN HOSTILE INTENT IS SUSPECTED, OR TAKEN HOSTAGE OR CAPTURED BY TERRORIST OR FOREIGN ACTOR ORGANIZATIONS. (LIMDIS/SIPR ONLY)	YES / PHONE	YES	0-4 HOURS	8A
22	SAFETY OF FLIGHT / USE MESSAGE GROUNDING / DEADLINING US ARMY EQUIPMENT IMPACTING OPNS / FLEET.	YES / E-MAIL	YES	0-4 HOURS	9
23	DIRECTED CHANGE IN FPCON BY OSD.	YES / PHONE	YES	0-4 HOURS	10

24	NATURAL OR MANMADE DISASTER IMPACTING US ARMY EQUITIES.	YES / E-MAIL	YES	0-4 HOURS	12
25	INCIDENT INVOLVING US ARMY PERSONNEL RESULTING IN NATIONAL POSITIVE OR NEGATIVE MEDIA COVERAGE.	YES / E-MAIL	YES	0-4 HOURS	14
26	INCIDENTS OF FRATRICIDE INVOLVING US ARMY PERSONNEL (BLUE ON BLUE / GREEN ON BLUE). (SIPR ONLY)	YES / PHONE	YES	0-4 HOURS	16
27	TRAINING OR TROOP MOVEMENT ACCIDENT/INCIDENT RESULTING IN DEATH OR VERY SERIOUS INJURY (E.G., LOSS OF LIMB, EYESIGHT, PARALYSIS, CRITICAL CONDITION, DISCOVERY OF AN ACUTE LIFE-THREATENING MEDICAL CONDITION). ADDITIONAL REPORTING REQUIRED ICW AR 190-45 CHAPTER 8.	YES / PHONE	YES	0-4 HOURS	18A
28	TRAINING OR TROOP MOVEMENT ACCIDENT/INCIDENT RESULTING IN A SERIOUS INJURY (E.G., AIR MEDICAL EVACUATION, HOSPITALIZATION, OR MEDICAL CONDITION CAUSING IMMEDIATE CONCERN BUT NO DANGER OF LOSS OF LIFE).	YES / PHONE	YES	0-4 HOURS	18B
29	NON-TRAINING ACCIDENT/INCIDENT RESULTING IN VERY SERIOUS INJURY (E.G., LOSS OF LIMB, EYESIGHT, PARALYSIS, CRITICAL CONDITION, DISCOVERY OF AN ACUTE LIFE THREATENING MEDICAL CONDITION) OF ARMY PERSONNEL.	YES / PHONE	YES	0-4 HOURS	24
30	THEFT, SUSPECTED THEFT, ATTEMPTED THEFT, LOSS, OR UNACCOUNTED ARMS, AMMUNITION, AND EXPLOSIVES (AA&E) OF ANY TYPE OR CALIBER; ANY FRAGMENTATION, CONCUSSION, OR HIGH EXPLOSIVE GRENADE, OR ANY EXPLOSIVE (E.G., C-4).	YES / E-MAIL	YES	0-4 HOURS	25A
31	ACTUAL OR ALLEGED CHILD ABUSE WHICH TAKES PLACE ON A US ARMY INSTALLATION / FACILITY (E.G., CDC, DOD SCHOOLS, ETC) OR WITHIN AN ARMY ORGANIZATIONAL SETTING IN WHICH THE VICTIM IS SEXUALLY ABUSED OR IS ADMITTED TO THE HOSPITAL DUE TO INJURIES INCURRED DURING THE INCIDENT (LIMDIS ONLY). ADDITIONAL REPORTING REQUIRED IN CONJUNCTION WITH AR 190-45 CHAPTER 8.	YES / PHONE	YES	0-4 HOURS	26
32	POTUS, FLOTUS, VPOTUS, SLOTUS, SGOTUS US GOVERNMENT SECRETARY, FOREIGN DIGNITARY, AMBASSADOR, OTHER US OR FOREIGN MILITARY SERVICE 4-STAR OR EQUIVALENT VISIT TO A US ARMY UNIT OR INSTALLATION.	YES / E-MAIL	YES	0-4 HOURS	28
33	INCIDENTS IN THE UNITED STATES, TERRITORIES, AND POSSESSIONS, INVOLVING ENGAGEMENT OF UA/UAS BY US ARMY EQUITIES IN FLIGHT, WITH THE INTENT TO DISRUPT OR DISABLE. REGARDLESS OF THE COUNTERMEASURE BEING EMPLOYED, THESE EVENTS MUST BE REPORTED TO FAA VIA PHONE NLT 5 MINUTES AFTER THE INCIDENT (TO ALLOW TIME TO DIVERT AIRCRAFT) FOLLOWED BY AN IMMEDIATE PHONE CALL TO THE AOC.(FAA COMMERCIAL PHONE: (540) 442-4423) (SEE REFERENCE L, FRAGO 4 FOR NOTIFICATION FORMAT) (SIPR ONLY)	YES / PHONE	YES	0-4 HOURS	31B
34	UA/UAS INCIDENTS INVOLVING US ARMY EQUITIES OUTSIDE THE UNITED STATES, TERRITORIES, AND POSSESSIONS, RESULTING IN C-UAS ENGAGEMENT; IMPACT TO MISSION; OR ANY INCIDENT DEEMED BY THE CDR NECESSARY TO REPORT. (SIPR ONLY)	YES / PHONE	YES	0-4 HOURS	31C
35	ANY ANOMALOUS HEALTH INCIDENTS (AHI) EVENT THAT TARGETS ARMY PERSONNEL.	YES / E-MAIL	YES	0-4 HOURS	32

Incident / Event	NOTIFY USAREC CG	REPORT TO HQDA AOC	USAREC ERP REPORTING TIME	DA CCIR#
USAREC SERIOUS INCIDENT REPORTING REQUIREMENTS (SIRs)				
36 COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS (C4) OUTAGES EXCEEDING 8 HOURS FOR BNS AND ABOVE. ALL USAREC ACTIVITIES WILL REPORT PLANNED AND UNPLANNED DEGRADATIONS OF C4 CAPABILITIES.	YES / E-MAIL	NO	0-12 HOURS	N/A
37 COMMUNICABLE ILLNESSES THAT EXCEED THE BASELINE FOR THOSE ILLNESSES AND UNUSUAL ILLNESSES. CONSULT WITH THE LOCAL MEDICAL TREATMENT FACILITY.	NO	NO	0-12 HOURS	N/A
38 ANY CHANGE TO FPCON OR CHANGES TO OTHER ALERT AND SECURITY STATUS LEVELS AFFECTING USAREC, SUBORDINATE ORGANIZATION, OR USAREC SUBORDINATE COMMAND INSTALLATIONS.	YES / PHONE	NO	0-12 HOURS	N/A
39 SUICIDE ATTEMPTS, EXHIBITING INDICATORS OF SERIOUS VIOLENT ACTS, OR SELF-INFLICTED POTENTIALLY INJURIOUS BEHAVIOR WITH A NONFATAL OUTCOME FOR WHICH THERE IS EVIDENCE (EITHER EXPLICIT OR IMPLICIT) OF INTENT TO DIE OF ANY MILITARY PERSONNEL, DEPENDENT, OR DA CIVILIANS ASSIGNED TO USAREC OR SUBORDINATE ORGANIZATIONS.	YES / E-MAIL	NO	0-12 HOURS	N/A
40 ANY REPORTED CASE OF RACISM OR RACIST ACTIVITY THAT RESULTS IN SERIOUS PHYSICAL INJURY, OR WHERE A SOLDIER, O4 AND E8 OR ABOVE OR DA CIVILIAN GS13 AND ABOVE IS THE SUBJECT.	YES / PHONE	NO	0-12 HOURS	N/A
41 SOLDIERS MISSING FROM PLACE OF DUTY ABSENT UNKNOWN (AUN), WHEREABOUTS UNKNOWN (DUSTWUN), OR ABSENT WITHOUT LEAVE (AWOL) .	YES / PHONE	NO	0-12 HOURS	N/A
42 SIGNIFICANT ENVIRONMENTAL INJURY TO A USAREC SOLDIER, DEPENDENT OR DA CIVILIAN THAT COULD IMPACT OR POTENTIAL IMPACT TRADOC MISSION (SUCH AS HEAT STROKE, RHABDOMYOLYSIS, CARBON MONOXIDE POISONING, HYPOTHERMIA, FROSTBITE, HEAT EXHAUSTION, AND COMMUNICABLE ILLNESS, SUCH AS INFLUENZA, HEPATITIS, AND WEST NILE VIRUS). CONSULT LOCAL MEDICAL FACILITY FOR ILLNESSES THAT EXCEED THE EXPECTED BASELINE.	YES / E-MAIL	NO	0-12 HOURS	N/A
43 SUSPECTED OR CONFIRMED INFORMATION SYSTEM INCIDENTS OR INTRUSIONS, PII BREACHES, INCIDENTS OR EVENTS TO BE REPORTED ARE DEFINED IN AR 25-2, PARA 4-21.2. THIS APPLIES TO ALL SOLDIERS AND CIVILIAN PERSONNEL ASSIGNED, ATTACHED, DETAILED, OR ON TEMPORARY DUTY WITH USAREC ORGANIZATIONS THAT CONTROL OR COLLECT PII.	NO	NO	0-12 HOURS	N/A
44 SERIOUS DOMESTIC VIOLENCE INCIDENTS (UNRESTRICTED REPORTING ONLY). RESULTING IN ARREST OR HOSPITALIZATION. SERIOUS DOMESTIC VIOLENCE IS DEFINED AS: "ANY INCIDENT OF DOMESTIC VIOLENCE WHERE A WEAPON (SUCH AS A FIREARM, KNIFE, OR MOTOR VEHILCE) IS INVOLVED; THE VICTIM SUFFERS A BROKEN LIMB, IS INJURED DURING PREGNANCY, IS SEXUALLY ABUSED, IS CHOKED OR STRANGLED OR IS ADMITTED TO THE HOSPITAL BECAUSE OF INJURIES INCURRED DURING THE INCIDENT; DOMESTIC VIOLENCE INCIDENTS WHERE A VIOLATION OF A PROTECTIVE ORDER (MILITARY OR CIVILIAN) HAS OCCURRED.	YES / PHONE	NO	0-12 HOURS	N/A
45 SERIOUS INJURY TO SOLDIER / DA CIVILIAN. (LIFE THREATENING) (LIFE/LIMB/EYE-SIGHT) ****VERY SERIOUSLY ILL/INJURED (VSI) OR SERIOUSLY ILL/INJURED (SI)	YES / PHONE	NO	0-12 HOURS	N/A
46 ANY ON / OFF-POST ARREST / MISCONDUCT OF PERMANENT PARTY (ANY COMMISSIONED OFFICER; MSG OR ABOVE; ANY WARRANT OFFICER; ARMY CIVILIAN GS-14 OR ABOVE).	YES / E-MAIL	NO	0-24 HOURS	N/A

47	ANY INCIDENT OF EXTREMISM, SUPREMACISM, AND GANG AFFILIATION ACTIVITIES INVOLVING SOLDIERS.					YES / E-MAIL	NO	0-24 HOURS	N/A
48	CURTAILMENT OF ACCESSIONS OPERATIONS (RECRUITING, MEPS CLOSURE, STATION CLOSURE, ROTC CAMPUS CLOSURE, IT SYSTEMS INOP).					NO	NO	0-24 HOURS	N/A
	Incident / Event					**NOTIFY USAREC CG**	**REPORT TO HQDA AOC**	**USAREC ERP REPORTING TIME**	**DA CCIR#**
USAREC INFORMATION REPORT (UIRS) (REPORTABLE TO USAREC ONLY)									
49	ARREST OF A SOLDIER OR DAC (MISDEMEANOR OR OFFENSE OTHER THAN A FELONY).					NO	NO	0-24 HOURS	N/A
50	DOMESTIC VIOLENCE / SPOUSE ABUSE / DOMESTIC ALTERCATION TO INCLUDE SOLDIER VICTIM (NOT A RESULTING OF HOSPITALIZATION).					YES / PHONE	NO	0-24 HOURS	N/A
51	CHILD ABUSE, CHILD NEGLECT, AND / OR CHILD ENDANGERMENT. **(ALSO SEE CCIR 31)**					NO	NO	0-24 HOURS	N/A
52	SEXUAL HARRASSMENT (NOT INVOLVING SUBJECTS OF RECRUITING EFFORTS).					NO	NO	0-24 HOURS	N/A
53	ADULTERY.					NO	NO	0-24 HOURS	N/A
54	DRUG OR ALCOHOL ABUSE (SELF REFERRAL, URINALYSIS, OR CHARGED).					NO	NO	0-24 HOURS	N/A
55	DUI/DWI.					NO	NO	0-24 HOURS	N/A
56	SUICIDAL IDEATION (THOUGHTS OF ENGAGING IN SUICIDE-RELATED BEHAVIOR).					NO	NO	0-24 HOURS	N/A
57	STRESS (CDHHE, SELF-REFERRAL, AND/OR HOSPITALIZATION).					NO	NO	0-24 HOURS	N/A
58	SEXUAL MISCONDUCT WITH SUBJECT OF RECRUITING EFFORTS (SRE DEFINED - ALL CONTACTS AND PROSPECTS (INCLUDES ALL HIGH SCHOOL STUDENTS REGARDLESS OF QUALIFICATION FOR MILITARY SERVICE), APPLICANTS, OR MEMBERS OF THE FSTP OR SISTER SERVICE EQUIVALENT ARE PROHIBITED). EXAMPLES OF MISCONDUCT: SEXTING, SOCIAL MEDIA, ETC... **(IF IT INVOLVES PHYSICAL CONTACT, SEE USAREC CG CCIR #6)**					NO	NO	0-24 HOURS	N/A
59	NATURAL DISASTER THAT WILL POTENTIALLY IMPACT USAREC PERSONNEL, FACILITIES, AND/OR PRODUCTION.					NO	NO	0-24 HOURS	N/A
60	THREATS MADE TO OR BY USAREC PERSONNEL (MILITARY OR CIVILIAN) OR PROPERTY.					NO	NO	0-24 HOURS	N/A
61	SUSPICIOUS ACTIVITY.					NO	NO	0-24 HOURS	N/A
62	DEMONSTRATIONS - AGAINST USAREC PERSONNEL OR CO-LOCATED FACILITIES.					NO	NO	0-24 HOURS	N/A
63	VANDALISM OF GOVERNMENT PROPERTY (RECRUITING STATIONS, GOVs, AND PROPERTY).					NO	NO	0-24 HOURS	N/A
64	GOV VEHICLE ACCIDENTS (PERSONNEL HOSPITALIZED).					NO	NO	0-24 HOURS	N/A
65	GOV VEHICLE THEFT TO INCLUDE LICENCE PLATES.					NO	NO	0-24 HOURS	N/A
66	LOSS OF A LAPTOP / CELL PHONE					NO	NO	0-24 HOURS	N/A
	Ledger:	**CG Priorities**	**HQDA**	**USAREC**	**USAREC COC WATCH OFFICER DESK: PHONE #: (502) 626-0823/0824/1455 HOURS OF OPERATION: WEEKDAYS: 0600-2400 HOURS; WEEKENDS/HOLIDAYS: CLOSED AFTER HOUR EMERGENCIES: CONTACT BILL SCHLETT AT (502) 974-4296**					

Appendix C – SIR Formats

Serious Incident Report (SIR) Report Format

CLASSIFICATION: CUI

SUBJECT: SIR number (BDE FYXX-XXX (Initial/Follow-up/Final))

1. Category (CCIR/PIR/Other):

2. Type of incident:

3. Date/time:
   a. DTG Incident:
   b. DTG BDE Notified:
   c. DTG 7Ws Submitted to HQs USACC:
   d. DTG DD3200 Signed (JROTC instructor misconduct):

4. Location of incident:

5. Other information:
   a. Racially Motivated:
   b. Alcohol involvement:
   c. Next of Kin (If death related):
      Name:
      Relationship:
      Address:
   d. Seatbelt use (Vehicle Mishaps):

6. Personnel involved:
   a. Subject(s)
      (1) Name:
      (a) Pay grade/MS Level:
      (b) DODID:
      (c) Race:
      (d) Sex:
      (e) Age:
      (f) Position:
      (g) Security Clearance:
      (h) Unit/School of assignment with address:
      (i) Duty Status:
         Cadre (AD/USAR/ARNG/DAC/Contractor)
         Cadet (Contracted/Green to Gold/SMP)
         JROTC Instructor/JROTC Student
         Student (Non-contracted, participating)
      (j) Was the Soldier flagged? Yes or No
      (k) Marital Status:

b. Victim(s):
(1) Name:
(a) Pay grade/MS Level:
(b) DODID:
(c) Race:
(d) Sex:
(e) Age:
(f) Position:
(g) Security Clearance:
(h) Unit/School of assignment with address:
(i) Duty Status:
Cadre (AD/USAR/ARNG/DAC/Contractor)
Cadet (Contracted/Green to Gold/SMP)
JROTC Instructor/JROTC Student
Student (Non-contracted, participating)
(j) Marital Status:

7. Summary of incident (initial):
a. Follow-up
b. Final

8. Remarks:
a. Initial Actions Taken by Unit:
b. Final Disposition:

9. Publicity (Expected, not expected):

10. Commander reporting:

11. Unit Point of contact:

12. Downgrading instructions: CUI protective markings will not be removed as this contains personally identifiable information.

Serious Incident Report (SIR) Report Format (SHARP)

CLASSIFICATION: CUI

SUBJECT: SIR number (BDE FYXX-XXX (Initial/Follow-up/Final))

1. Category (CCIR/PIR/Other):

2. Type of incident:

3. Date/time:
   a. DTG Incident:
   b. DTG BDE Notified:
   c. DTG 7Ws Submitted:
   d. SHARP ONLY: DTG DD 2910 was signed (if eligible):

4. Location of incident:

5. Other information:
   a. Racially Motivated:
   b. Alcohol involvement:
   c. Next of Kin (If death related):
      Name:
      Relationship:
      Address:
   d. Seatbelt use (Vehicle Mishaps):

6. Personnel involved:
   a. Subject(s) Provide all information. WILL BE REDACTED BY G3)
      (1) Name:
      (a) Pay grade/MS Level:
      (b) DODID:
      (c) Race:
      (d) Sex:
      (e) Age:
      (f) Position:
      (g) Security Clearance:
      (h) Unit/School of assignment with address:
      (i) Duty Status:
         Cadre (AD/USAR/ARNG/DAC/Contractor)
         Cadet (Contracted/Green to Gold/SMP)
         JROTC Instructor/JROTC Student
         Student (Non-contracted, participating)
      (j) Was the Soldier flagged? Yes or No
      (k) Marital Status:

   b. Victim(s): (Provide all information. WILL BE REDACTED BY G3)
      (1) Name:

(a) Pay grade/MS Level:
(b) DODID:
(c) Race:
(d) Sex:
(e) Age:
(f) Position:
(g) Security Clearance:
(h) Unit/School of assignment with address:
(i) Duty Status:
Cadre (AD/USAR/ARNG/DAC/Contractor)
Cadet (Contracted/Green to Gold/SMP)
JROTC Instructor/JROTC Student
Student (Non-contracted, participating)
(j) Marital Status:

7. Summary of incident (initial): (Complete details of events EXCEPT SHARP)
SHARP ONLY:

- Sexual Assault: must include type of Sexual Assault, what crime is being investigated. do NOT include specific details of the assault. (Per AR 600-20, appendix J-2)

- Sexual Harassment: What type of sexual harassment (quid pro quo and/or hostile environment), do not include specific details of harassment.

a. Follow-up
SHARP ONLY- Required if SUBJECT involved belongs to USACC
b. Final

8. Remarks:

a. Initial Actions Taken by Unit: SHARP ONLY: Response to date (example, USACIDC investigation initiated with case number, appointment of an investigating officer, suspense of a commander, suspension/revocation of a SHARP professional's appointment orders, MPO/CPO put in place, separation of Victim/Alleged Offender, Alleged Offender flag and security clearance suspension).

b. Final Disposition:

c. SHARP ONLY: Other factors (example, AO removed from leadership position, known or expected media or international interest, safety of victim, or any other pertinent information regarding the victim's well-being)

9. Publicity (Expected, not expected):

10. Commander reporting:

11. Unit Point of contact:

12. BDE SHARP Point of contact (SARC/VA): for SHARP related reports

13. Downgrading instructions: CUI protective markings will not be removed as this contains personally identifiable information.

Appendix D – DR Format

Disaster Report (DR) Format

Disaster reports are sent as an unencrypted email.

Named Disaster/Storm:

Date/time of report:

BDE-Unit:

1. Actions Taken:

2. Accountability of personnel: (accounted for/assigned)
    a. Cadre: #/#
    b. Cadet: #/#
    c. Dependents in the local area: #/#

3. Displaced and Evacuated Personnel by Category (CAT) see descriptions page 2. Provide, in slant format by category, the total number of displaced persons (MIL/DAC/DEP) within your command.
    a. CAT 1: MIL/DAC/DEP
    b. CAT 2: MIL/DAC/DEP
    c. CAT 3: MIL/DAC/DEP
    d. Mandatory evacuation order issued by local officials:
        1) location

4. Impact on
    a. Training/Campus Activities- i.e. Closures/Damages
    b. Facility damage/equipment loss
    c. Home damage

5. Current Local Weather:

6. Any service or assistance provided to other units/services- i.e. NG or RES activations
    a. CADRE:
    b. CADET:

7. Any support required from HHQ

Displaced Category Definitions

Category 1 Displaced Persons. CAT 1 Displaced Persons are defined as those Military, DA Civilian, and dependents who are displaced from their primary duty residence AND primary duty location. This includes people under mandatory evacuation orders, conditions preventing safe return (weather effects or destruction/damage to residences/duty locations), or other situations identified by commands that prevent these personnel from returning to their homes and places of primary duty.

Category 2 Displaced Persons. CAT 2 Displaced Persons are defined as those Military, DA Civilian, and dependents who are displaced from their primary duty location but remain at their primary duty residence. This includes, but is not limited to, personnel that were not evacuated from the affected area (remain at their primary duty residence) but are not able to report for duty. This includes, but is not limited to, personnel unable to safely report for duty due to damage and weather effects. This does not include personnel ordered by commands not to report for duty for administrative purposes such as installation under reduced operations (key and essential personnel only).

Category 3 Displaced Persons. CAT 3 Displaced Persons are defined, for the purpose of this order, as those Military, DA Civilian, and dependents who are displaced from their primary duty residence but are able to return to their primary duty location. This includes, but is not limited to, personnel evacuated from the affected area that are able to safely report for normal duty.

	Displaced Residence	Displaced Duty Station
CAT 1	**YES**	**YES**
CAT 2	**NO**	**YES**
CAT 3	**YES**	**NO**

SUSPICIOUS ACTIVITY REPORT

See USACC SOP 23-11 for use of this form. The proponent agency is USACC G3.

Terrorist and criminal operations can begin with extensive planning. Reporting suspicious activity can help mitigate or prevent an attack or crime. USACC SOP 23-11 and USACC OPLAN Vigilance address suspicious activity reporting. USACC Personnel will report suspicious activities via the Incident Reporting SOP or directly to the USACC G3 Protection Division at usaccprotectiondivision@army.mil.

Instructions: Fill out the blocks to the best of your knowledge. Blocks marked with an * are required.

PART I: GENERAL INFORMATION

1. Date Activity Observed:*	2. Time Activity Occurred:*	3. Reporting Unit:*

4. Suspicious Activity Location and Address:	5. Name of Facility:

6. Reporter's Name:*	7. Rank:	8. Phone Number:*	9. Email Address:*

10a. Was Law Enforcement Contacted?*	10b. If answer to 10a is yes, enter Agency Contact Info:	10c. Unit Report Number:
☐ Yes ☐ No		

PART II: SUSPICOUS ACTIVITY INFORMATION

11. Indicators:* Indicators listed below help identify suspicious activity behavior. Check any that apply and provide detailed narrative of the activity in Block 12. Include additional indicator information in blocks 13-14 on suspicious vehicle descriptions and blocks 15-16 on suspicious person descriptions.

☐ Surveillance	☐ Eliciting Information	☐ Tests of Security
☐ Acquisition of Expertise	☐ Material Acquisition or Storage	☐ Theft, Loss or Diversion
☐ Misrepresentation	☐ Expressed or Implied Threat	☐ Recruiting
☐ Sabotage, Tampering or Vandalism	☐ Weapons Discovery	☐ Breach/Attempted Intrusion
☐ Flyover/Landing	Other:	

12. Narrative of the Observed Activity (Who, what, when, where, why). Continuation block on page 2 if necessary:*

13. Suspicious Vehicle Information (if applicable):

Year:

Direction of Travel:

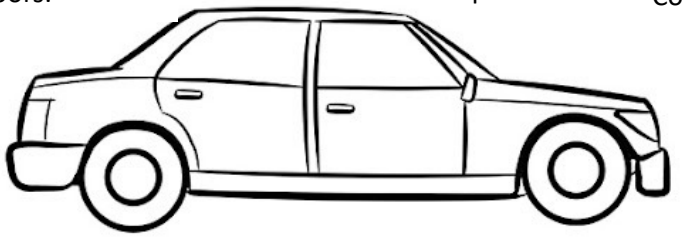
Make:

Model:

# of Doors:

No of Occupants:

Color:



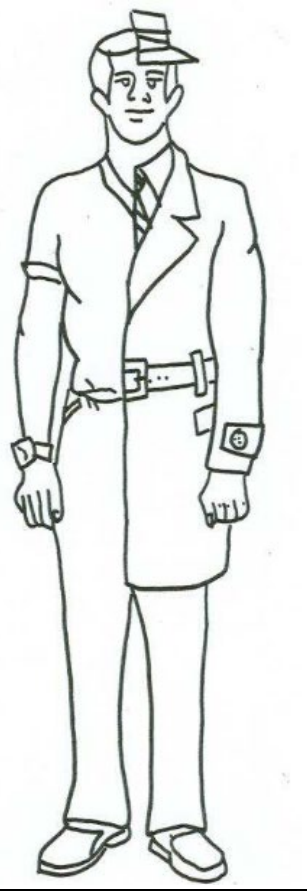
License Plate#:

Note if any or all lights are operational:

14. Additional Information:

15. Suspicious Person Description (Provide as much information about suspicious persons as possible):

Sex:	Race:	Age:	Height:	Weight:	Weapon:

Hair Color:		Hat:
Glasses Type:		Tie:
Complexion:		Shirt:
Scars/Marks:		Coat:
Tattoos:		Pants:
		Shoes:

16. Additional information about suspicious persons:

17. Continuation Section:

Appendix F – PII Breach Report

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

F-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 F-1 and F-2 for a sample of a completed DD Form 2959 and a sample USAREC center/activity Breach Report PII Flow Chart. See the USAREC Privacy Act/PII Reporting site at http://www.USAREC.army.mil/PrivacyAct.asp.

F-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 responsible person.

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.

F-3. Notification procedures

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

a. The USACC organization that had responsibility to control access to the compromised PII must notify affected individuals deemed at high risk of identity theft. USACC 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, CAC-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 USACC command/activity should not notify personnel of breaches that have a low overall likelihood of harm. USACC 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 USACC 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 chief) 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.

e. When the sender is not acquainted with the affected individuals, the commander/chief 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.

F-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 reinforce 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

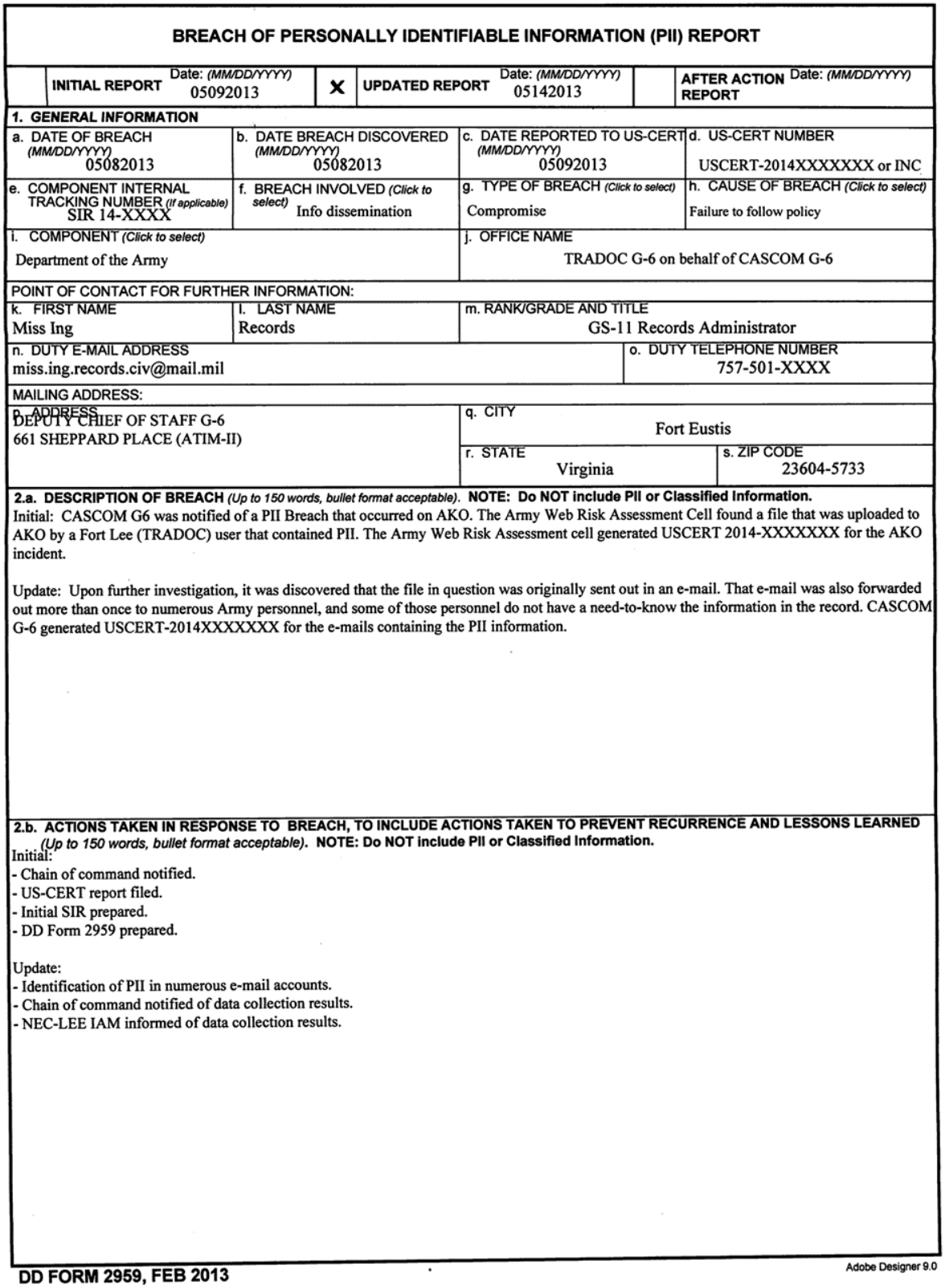
managerial training and videos, for remedial training.

F-5. Identity theft risk analysis

Commanders/chiefs 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.

a. 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.

b. Low and moderate risk/harm determinations and the decision whether notification of the individuals is made rest with the head of the USAREC organization where the breach occurred. All determinations of high risk/harm require notification. USAREC 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.



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)	b. DATE BREACH DISCOVERED (MM/DD/YYYY)	c. DATE REPORTED TO US-CERT (MM/DD/YYYY)	d. US-CERT NUMBER
05082013	05082013	05092013	USCERT-2014XXXXXXX or INC
e. COMPONENT INTERNAL TRACKING NUMBER (If applicable)	**f. BREACH INVOLVED (Click to select)**	**g. TYPE OF BREACH (Click to select)**	**h. CAUSE OF BREACH (Click to select)**
SIR 14-XXXX	Info dissemination	Compromise	Failure to follow policy

i. COMPONENT (Click to select)	j. OFFICE NAME
Department of the Army	TRADOC G-6 on behalf of CASCOM G-6

POINT OF CONTACT FOR FURTHER INFORMATION:

k. FIRST NAME	l. LAST NAME	m. RANK/GRADE AND TITLE
Miss Ing	Records	GS-11 Records Administrator

n. DUTY E-MAIL ADDRESS	o. DUTY TELEPHONE NUMBER
miss.ing.records.civ@mail.mil	757-501-XXXX

MAILING ADDRESS:

p. ADDRESS	q. CITY	r. STATE	s. ZIP CODE
DEPUTY CHIEF OF STAFF G-6 661 SHEPPARD PLACE (ATIM-II)	Fort Eustis	Virginia	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-XXXXXXX 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-2014XXXXXXX for the e-mails containing the PII information.

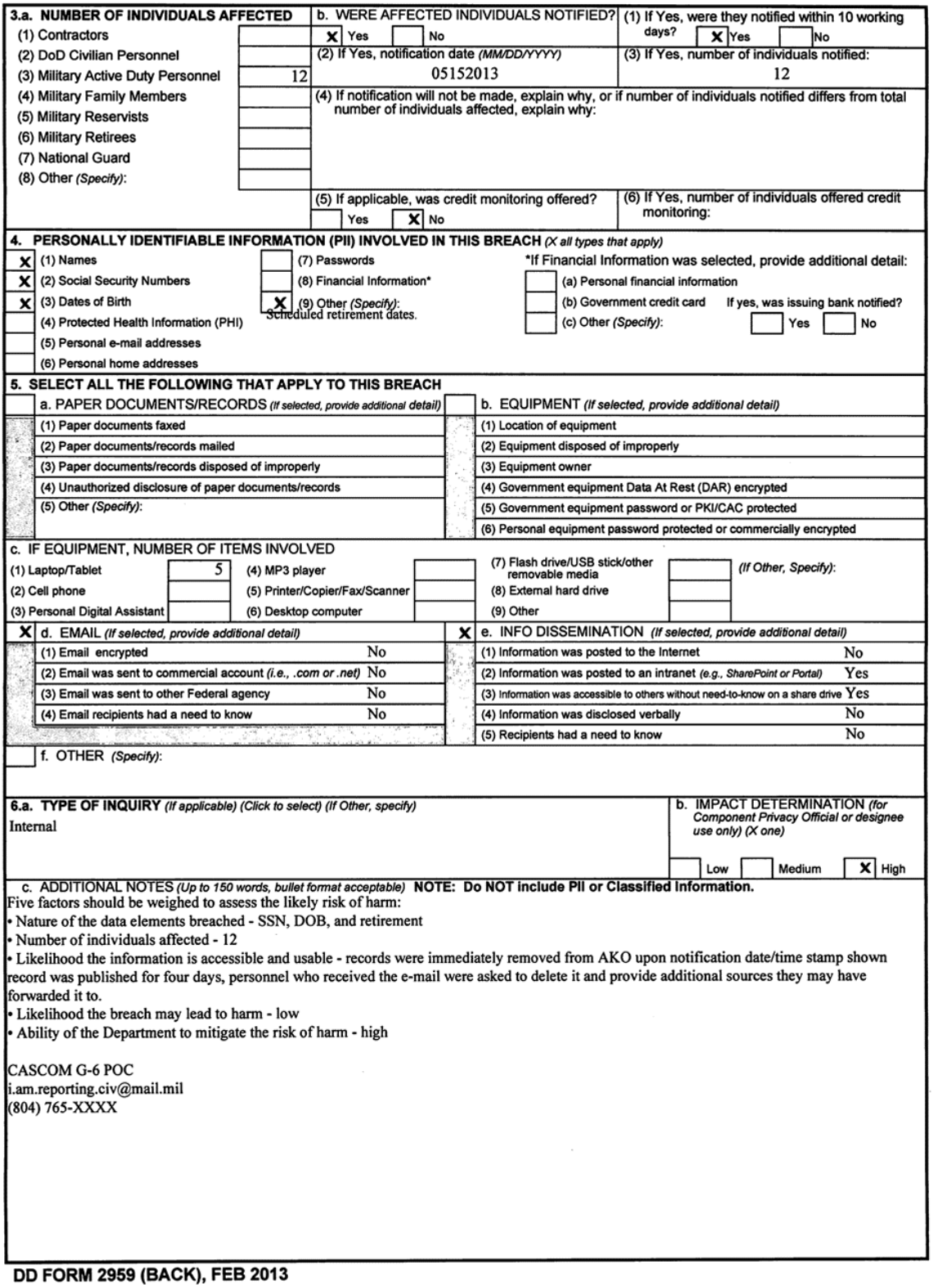
2.b. ACTIONS TAKEN IN RESPONSE TO BREACH, TO INCLUDE ACTIONS TAKEN TO PREVENT RECURRENCE AND LESSONS LEARNED *(Up to 150 words, bullet format acceptable).* **NOTE: Do NOT include PII or Classified Information.**

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 F-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	12
(4) Military Family Members	
(5) Military Reservists	
(6) Military Retirees	
(7) National Guard	
(8) Other *(Specify)*:	

b. WERE AFFECTED INDIVIDUALS NOTIFIED? [X] Yes [ ] No

(1) If Yes, were they notified within 10 working days? [X] Yes [ ] No

(2) If Yes, notification date *(MM/DD/YYYY)*: 05152013

(3) If Yes, number of individuals notified: 12

(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? [ ] Yes [X] No

(6) If Yes, number of individuals offered credit monitoring:

4. PERSONALLY IDENTIFIABLE INFORMATION (PII) INVOLVED IN THIS BREACH *(X all types that apply)*

- [X] (1) Names
- [X] (2) Social Security Numbers
- [X] (3) Dates of Birth
- [ ] (4) Protected Health Information (PHI)
- [ ] (5) Personal e-mail addresses
- [ ] (6) Personal home addresses
- [ ] (7) Passwords
- [ ] (8) Financial Information*
- [X] (9) Other *(Specify)*: Scheduled retirement dates.

*If Financial Information was selected, provide additional detail:

- [ ] (a) Personal financial information
- [ ] (b) Government credit card — If yes, was issuing bank notified? [ ] Yes [ ] No
- [ ] (c) Other *(Specify)*:

5. SELECT ALL THE FOLLOWING THAT APPLY TO THIS BREACH

a. PAPER DOCUMENTS/RECORDS *(If selected, provide additional detail)* [ ]

- (1) Paper documents faxed
- (2) Paper documents/records mailed
- (3) Paper documents/records disposed of improperly
- (4) Unauthorized disclosure of paper documents/records
- (5) Other *(Specify)*:

b. EQUIPMENT *(If selected, provide additional detail)* [ ]

- (1) Location of equipment
- (2) Equipment disposed of improperly
- (3) Equipment owner
- (4) Government equipment Data At Rest (DAR) encrypted
- (5) Government equipment password or PKI/CAC protected
- (6) Personal equipment password protected or commercially encrypted

c. IF EQUIPMENT, NUMBER OF ITEMS INVOLVED

(1) Laptop/Tablet	5	(4) MP3 player		(7) Flash drive/USB stick/other removable media		*(If Other, Specify)*:
(2) Cell phone		(5) Printer/Copier/Fax/Scanner		(8) External hard drive		
(3) Personal Digital Assistant		(6) Desktop computer		(9) Other		

d. EMAIL *(If selected, provide additional detail)* [X]

- (1) Email encrypted — No
- (2) Email was sent to commercial account *(i.e., .com or .net)* — No
- (3) Email was sent to other Federal agency — No
- (4) Email recipients had a need to know — No

e. INFO DISSEMINATION *(If selected, provide additional detail)* [X]

- (1) Information was posted to the Internet — No
- (2) Information was posted to an intranet *(e.g., SharePoint or Portal)* — Yes
- (3) Information was accessible to others without need-to-know on a share drive — Yes
- (4) Information was disclosed verbally — No
- (5) Recipients had a need to know — No

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)*: [ ] Low [ ] Medium [X] 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 F-1. Sample DD Form 2959, cont.

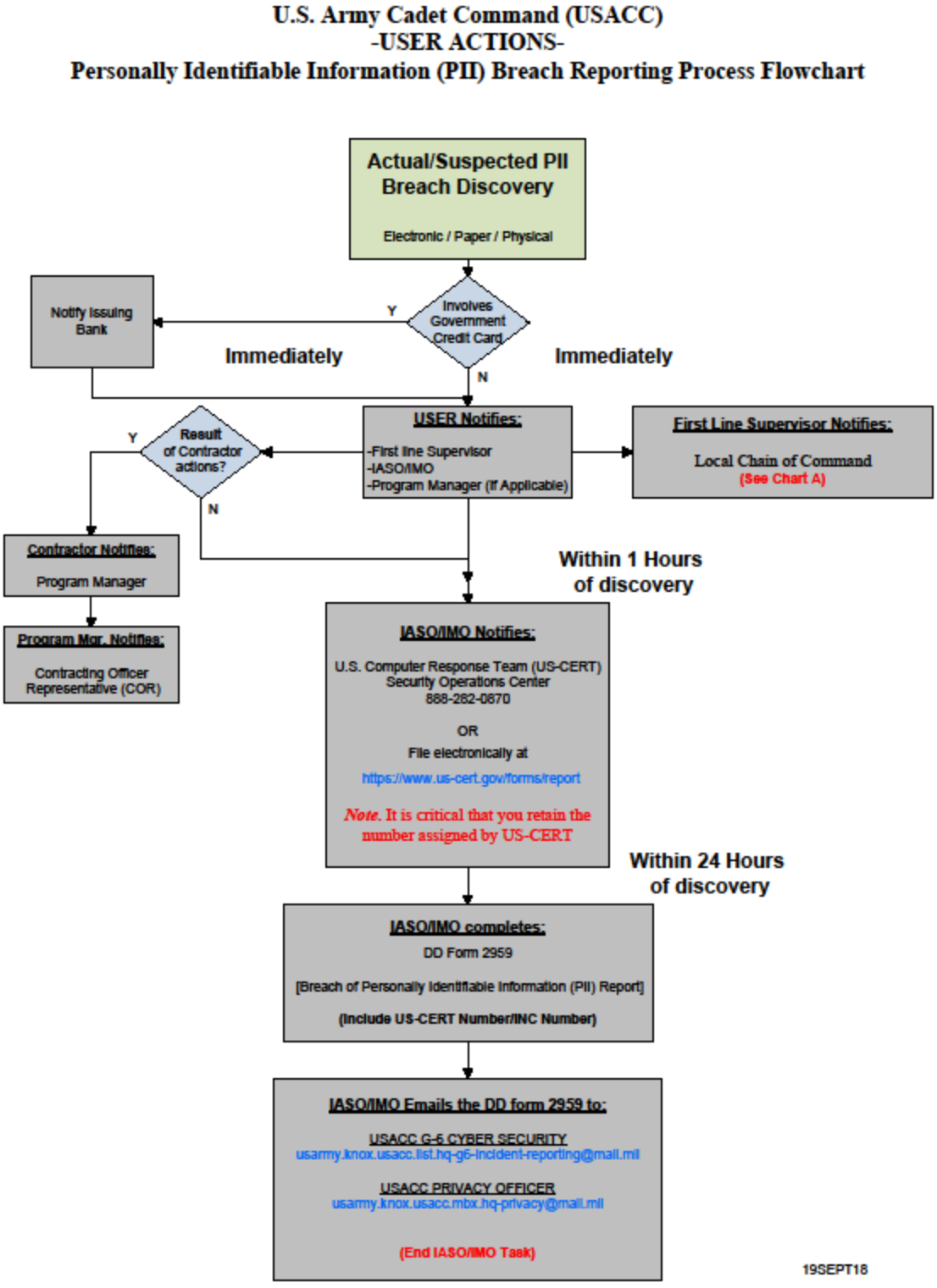


Figure F-2. Sample USACC center/activity Breach Report PII Flowchart

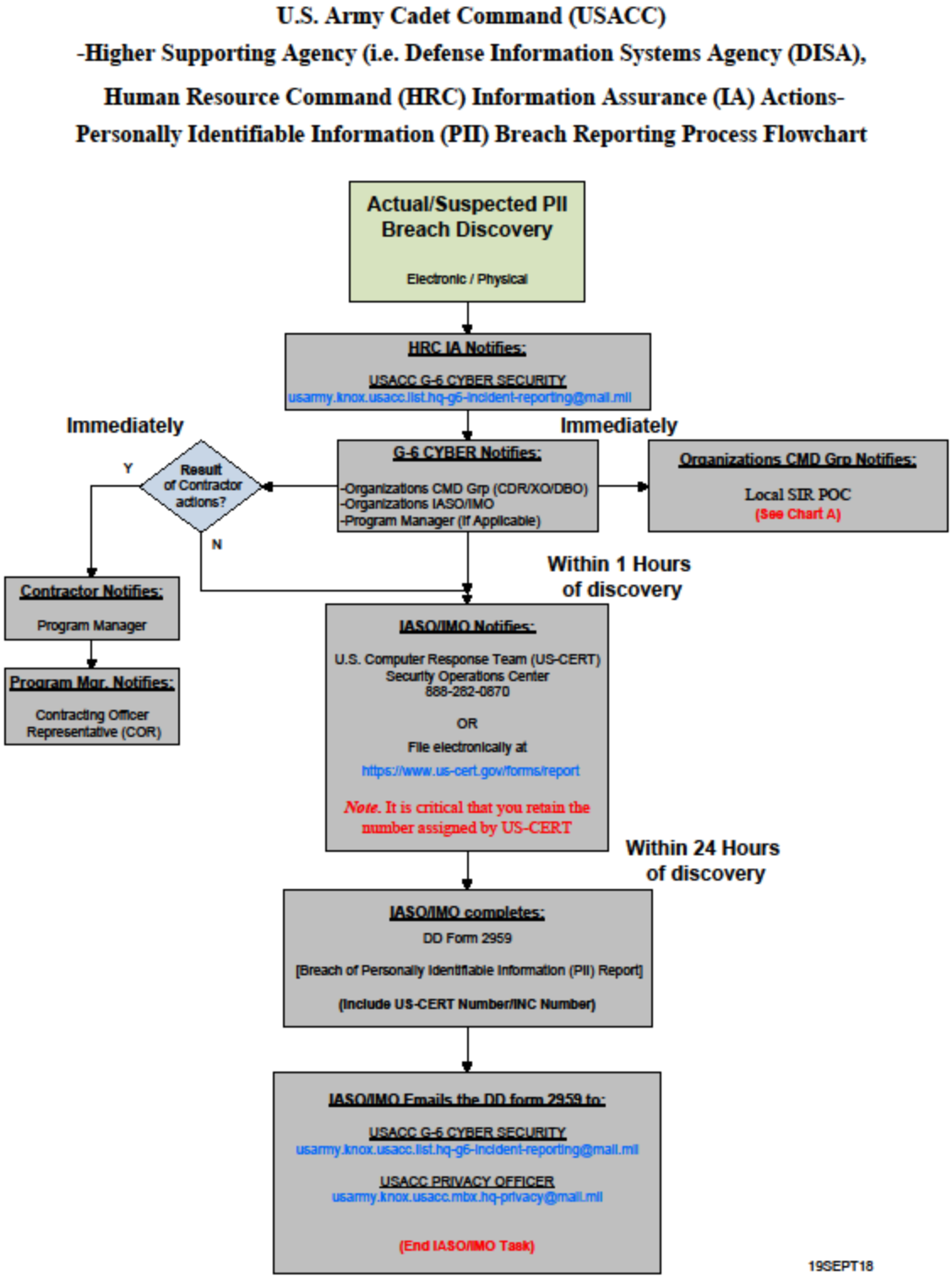


Figure F-2. Sample USACC center/activity Breach Report PII Flowchart, cont.

U.S. Army Cadet Command (USACC)
-CHAIN OF COMMAND ACTIONS-
Personally Identifiable Information (PII) Breach Reporting Process Flowchart

Chart A

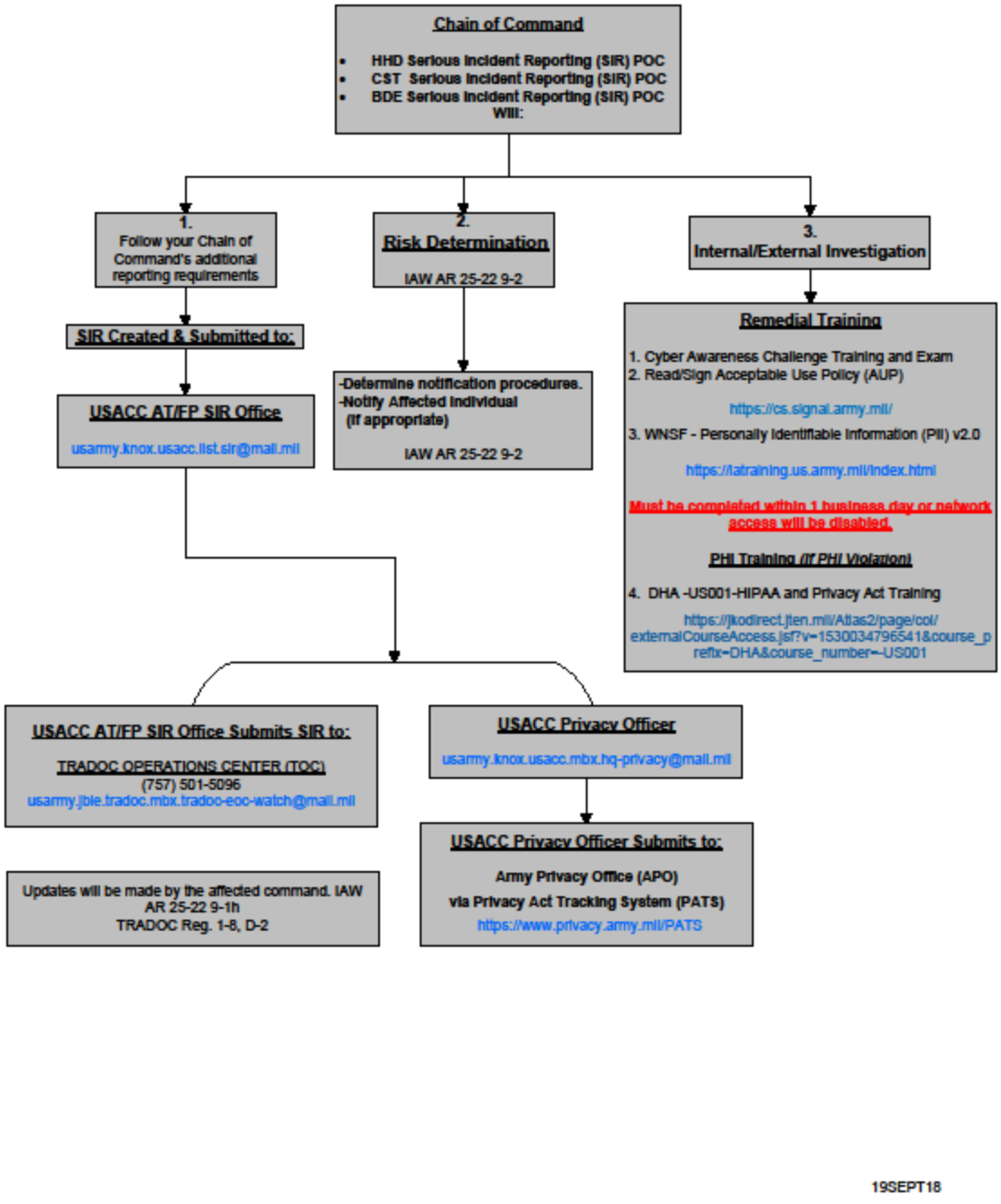


Figure F-2. Sample USACC center/activity Breach Report PII Flowchart, cont.

Appendix G – Management Control Checklist

Management Control Checklist

G-1. Function

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

G-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.

G-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.

G-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 HHQ immediately upon discovery or notification?

c. Are initial written SIRs sent to the USACC SIR POC within 24 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 USACC SIR POC?

g. Are SARs used in accordance with this SOP?

h. Are SARs submitted to the USACC SIR POC within reasonable timeframe of knowledge of the incident?

i. Does the USACC staff conduct trend analysis and provide feedback on identified trends to the USACC leadership on a routine basis?

G-5. Suppression

No previous management control evaluation checklist exists for this program.

G-6. Comments

Help to make this a better tool for evaluating management controls. Submit comments directly to Operations Division (G-3), Chief.

Appendix H – RFI Format

USACC SIR Request for Information format

1. SIR Reference Number		**2. Suspense DTG**	
3. Requesting Agency/Directorate			
4. Required Information	***(Be as specific as possible)***		
5. Justification For Information Request	***(State clearly the reason(s) information is required)***		
6. Name and Contact Information of Requestor	***(Include phone numbers and email address)***		
7. BDE/BN POC Reply	(***BDE/BN POC will use this area to answer requested information. DO NOT SUPPLY ADDITIONAL INFORMATION. Answer only those questions asked as specifically as possible)***		
8. Name and Contact Information of BDE/BN POC	***(Include phone numbers and email address)***		

- Requesting Agencies/Directorates must forward RFI through the USACC POC'S
- BDE/BN POCs will answer RFI in Block 7 and forward reply to the USACC POC'S using encrypted email.
- The USACC POC will process the reply and forward to the requesting agency/directorate using encrypted email.

Appendix I – Glossary

Section I
Abbreviations

ACoS
Assistant Chief of Staff

AD
Active Duty

ADO
Active Duty Option

AR
Army regulation

ARNG
Army National Guard

C4
Command, Control, Communications, and Computers

CAC
Common Access Card

CAT
Category

CCIR
Commander's Critical Information Requirement

CDT
Cadet

CG
Commanding General

CID
Criminal Investigation Division

COC
Command Operations Center

COS
Chief of Staff

CST
Cadet Summer Training

CUI
Controlled Unclassified Information

DA
Department of the Army

DAC
Department of the Army Civilian

DAMO-ODO
Department of the Army Management Office of Operations and Contingency Planning

DA PAM
DA Pamphlet

DCS
Deputy Chief of Staff Office (i.e. DCS G3, DCS G1, etc.)

DD Form
Department of Defense Form

DEP
Dependent

DOD
Department of Defense

DR
Disaster Reports

DSAID
Defense Sexual Assault Incident Database

DSN
Defense Switched Network

DTG
Date/Time Group

DUI
Driving Under the Influence

EOC
Emergency Operations Center

ERP
Electronic Reporting Portal

FFIR
Friendly Force Information Requirements

FOUO
For Official Use Only

FPCON
Force Protection Condition

G2G
Green to Gold

HHQ
Higher Headquarters

HIPAA
Health Insurance Portability and Accountability Act

HQ
Headquarters

IAW
In Accordance With

IOC
Installation Operations Center

IR
Incident Reports

JROTCI
Junior Reserve Officer Training Corps Instructor

JTTF
Joint Terrorism Task Forces

NIPRNET
Non-secure Internet Protocol Router network

NIST
National Institute of Standards and Technology

PII

Personally Identifiable Information

PIR
Priority Intelligence Requirements

PMO
Provost Marshal Office

POC
Point of Contact

RFI
Request For Information

ROTC
Reserve Officer Training Corps

SAR
Suspicious Activity Report

SARC
Sexual Assault Response Coordinator

SC
Senior Commander

SHARP
Sexual Harassment/Assault Response & Prevention

SIPRNET
Secure Internet Protocol Router Network

SIR
Serious Incident Report

SMP
Simultaneous Membership Program

SROTC
Senior Reserve Officers' Training Corps

SSN
Social Security Number

TRADOC
U.S. Army Training and Doctrine Command

USACID
U.S. Army Criminal Investigation Division

U.S.
United States

USACC
U.S. Army Cadet Command

USACIDC
U.S. Army Criminal Investigation Division Command

USAR
United States Army Reserve

USAREC
U.S. Army Recruiting Command

Section II
Terms

Abusive Sexual Contact
By threatening or placing that other person in fear. That the accused committed sexual contact upon or by another person; and that the accused did so by threatening or placing that other person in fear.

Aggravated Sexual Contact
By force. That the accused committed sexual contact upon or by another person; and that the accused did so with unlawful force. By force causing or likely to cause death or grievous bodily harm.

At Echelon
Incidents that are reportable to the next level of command only (i.e. SROTC Program to Brigade, Brigade to HQs, etc.)

Bomb Threat
Communication of any kind to use a bomb.

Cadet
- Contracted Cadet – A contracted Cadet is a student who has been determined eligible for enrollment (signed CC Form 139-R) and signed a DA Form 597/597-3 as applicable and the DD Form 4 series. Contracted Cadets are enrolled in the SROTC program as non-scholarship or scholarship Cadets. Completion Cadets remain contracted Cadets.
    - Green 2 Gold Active-Duty Option (ADO) – Program for Regular Army Soldiers who remain on active duty while attending college.

- Green 2 Gold (Scholarship/Non-Scholarship) – Program for Regular Army Soldiers who are discharged early in order to pursue a 2–4-year college degree and ROTC.
- Simultaneous Membership Program (SMP) – Program that provides for concurrent enrollment in the ROTC Advanced Course and enlisted membership in an ARNG or USAR troop program.

- Non-Contracted Cadet – Non-contracted Cadets are students who have completed and signed the CC Form 139-R but have not completed/signed the DA FM 597/597-3 or the DD FM 4 Series. The non-contracted Cadet category includes students with a scholarship award pending contracting, advanced designee scholarship awardees, immigrant aliens/refugees, and non-scholarship conditional Cadets who have completed and signed the CC Form 139-R and DA FM 597.

Cadre
Military (AD, RES, NG), Civilian (DAC/Contractor) assigned or attached to USACC performing duties in support of the USACC mission.

Elicitation
Any attempts to obtain security-related or military specific information by anyone who does not have the appropriate security clearance and need to know.

Ideations
Verbal or non-verbal expressions of suicide considerations.

Immediate Family Member
Includes those individuals for whom a Subject 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. For cadets, immediate family includes the parent/guardian or siblings of the cadet.

Non-specific Threat
Threats received by any means, to include time, location, or area for an attack against US forces, facilities, or mission.

Quid pro Quo
This for that.

Rape
By unlawful force, that the accused committed a sexual act upon another person; and that the accused did so with unlawful force. By force causing or likely to cause death or grievous bodily harm.

Repetitive Activities
An activity that has occurred two or more times by the same person and or vehicle within a 1-month period.

Self-harm (without intent to die)
A self-inflicted, potentially injurious behavior for which there is evidence (either explicit or implicit) that the person did not intend to kill himself/herself (i.e., had no intent to die).

Sexual Assault
By threatening or placing that other person in fear; that the accused committed a sexual act upon another person; and that the accused did so by threatening or pacing that other person in fear.

Stress
Observed stress or request for help without actions.

Suicide Attempts (includes intent to die)
Self-inflicted potentially injurious behavior with a nonfatal outcome for which there is evidence (either explicit or implicit) of intent to die.

Suicidal ideation (only without an attempt)
Any self-reported thoughts of engaging in suicide-related behaviors.

Surveillance
Any reported possible surveillance in which an attempt to record information or to use unusual means to monitor activities is observed.

Suspicious Activities/Incidents
Should only be used if the reportable information DOES NOT meet any of the above criteria, but is believed to represent a force protection threat, then it should be reported under this category.