DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
3800 NORTH CAMP CREEK PARKWAY SW
ATLANTA, GA 30331-5099
1 August 1995

USARC Regulation 380-3

Security

SAFEGUARDING AND CONTROL OF COMMUNICATIONS SECURITY (COMSEC) MATERIAL

History. This is the initial publication of USARC Regulation 380-3.

Summary. This regulation prescribes policies and procedures for the safeguarding and control of COMSEC material.

Applicability. This regulation applies to Headquarters, U.S. Army Reserve Command (USARC) and its direct reporting activities. Local reproduction is authorized.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, Intelligence (DCSINT). The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. Proponents may delegate this approval authority, in writing, to a division chief under their supervision within the proponent agency in the grade of colonel or the civilian equivalent.

Supplementation. Supplementation of this regulation is prohibited without prior approval from Commander, USARC, ATTN: AFRC-IN, 3800 North Camp Creek Parkway SW, Atlanta, GA 30331-5099.

DISTRIBUTION: B

Interim changes. Interim changes to this regulation are not official unless authenticated by the Deputy Chief of Staff, Information Management (DCSIM). Users will destroy interim changes on their expiration date unless superseded or rescinded.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Commander, USARC, ATTN: AFRC-IN, 3800 North Camp Creek Parkway SW, Atlanta, GA 30331-5099.

FOR THE COMMANDER:

OFFICIAL:

ROBERT S. HARDY, JR.
Brigadier General
Chief of Staff

SIGNED
CAROLYN E. RUSSELL
Colonel, GS
Deputy Chief of Staff,
Information Management

Contents *(Listed by paragraph number)*

1. Purpose

This regulation prescribes policies and procedures for management of U.S. Army Reserve Command (USARC) Communication Security (COMSEC) accounts, to include the safeguarding and control of COMSEC material. Submit requests for exception to policy contained in this regulation, in writing, to Commander, USARC, ATTN: AFRC-INS.

2. References

a. Required publications.

(1) AR 190-51 (Security of Unclassified Army Property (Sensitive and Non-Sensitive). Cited in paragraph 10, figure 1.

(2) AR 380-5 (Department of the Army Information Security Program). Cited in paragraphs 4d(1), 7, 8b, figure 1, A-8, A-34, and B-3.

(3) AR 380-19 (Information System Security). Cited in paragraphs 6c and 8.

(4) AR 380-40 (Department of the Army Policy for Safeguarding and Controlling COMSEC Information). Cited in paragraphs 4c(4)(b) and (d), 4d(1), 4e, 10, 11d(5)(d), figure 1, appendix A, and B-1.

(5) DA Pam 25-380-2 (Security Procedures for Controlling Cryptographic Items). Cited in paragraphs 6c, 8, and 10.

(6) TB 380-41 (Procedures for Safeguarding, Accounting and Supply of COMSEC Material). Cited in paragraphs 4d, 4e, 8, 9a, 10, figure 1, appendix A, B-1, and B-2a(11).

b. Related publications.

(1) AR 15-6 (Procedures for Investigating Officers and Boards of Officers).

(2) AR 25-12 (Communications Security Equipment Maintenance and Maintenance Training).

(3) AR 25-400-2 (The Modern Army Recordkeeping System (MARKS))

(4) AR 380-53 (Communications Security Monitoring).

c. Recordkeeping requirements. This regulation requires the creation, maintenance, and use of the following specific records: File Number 380-5a, Cryptographic Access Authorization and Termination (USARC Forms 65-R).

3. Explanation of abbreviations

Abbreviations used in this regulation are explained in the glossary.

4. Responsibilities

a. The USARC DCSINT will --

(1) Prescribe policy and procedures for safeguarding and controlling COMSEC material.

(2) Establish and maintain a Command COMSEC Inspection Program.

(3) Approve, in coordination with Deputy Chief of Staff, Operations (DCSOPS), all requests for the establishment of COMSEC accounts.

(4) Ensure that all COMSEC incidents are properly and promptly reported within the Command.

b. The USARC DCSIM will--

(1) Appoint in writing a minimum of one individual as a COMSEC Inspector.

(2) Conduct Command COMSEC Inspections of all regional support commands (RSC), direct reporting commands (DRC), USARC installations and Regional Training Sites. Inspections will not exceed an interval of 24 months.

(3) Approve, in coordination with DCSINT, all requests for initial key material.

(4) Act as command authority on security telephone unit, third generation (STU-III) and Reserve Component Automation System (RCAS) keys.

(5) Establish procedures for the requisition and control of STU-III key.

(6) Establish procedures for the requisition and control of RCAS key.

(7) Monitor, in coordination with DCSINT, all Cryptographic Evaluation Reports (CER) from controlling authorities (CONAUTH) that support USARC COMSEC accounts.

c. Commanders, RSCs and DRCs will--

(1) Ensure that all COMSEC custodians, alternates, and COMSEC inspectors successfully complete the Standardized COMSEC Custodian Course (SCCC) prior to appointment.

(2) Appoint, in writing, an experienced COMSEC custodian as the COMSEC Command Inspector.

(3) Establish a Command COMSEC Inspection Program for all COMSEC accounts under their jurisdiction. Such inspections will not exceed an interval of 12 months.

(4) Ensure that commanders at all levels--

(a) Appoint a qualified custodian and one alternate for each COMSEC account under their jurisdiction. Accounts that hold two-person control (TPC) material require a minimum of four alternates. For two-person integrity (TPI) material, two alternates are recommended.

(b) Ensure the Management Control Evaluation Checklist, DA Form 11-2-R, is completed by a command representative (other than the COMSEC custodian) in accordance with AR 380-40, appendix D. The COMSEC custodian will file the completed checklist within the account.

(c) Ensure that the unit COMSEC custodian promptly prepares and forwards replies to inspection deficiencies through command channels.

(d) Ensure that COMSEC users comply with the responsibilities prescribed in AR 380-40, paragraph 1-4i.

(e) Ensure that the unit COMSEC custodians complete the Semi-Annual Inventory Reports (SAIR), RCS AMC 877, as directed by Director, USACCSLA.

(f) Ensure that the unit COMSEC custodian promptly answers correspondence received from Director, USACCSLA. For USAR activities, 60 days is sufficient time to meet suspense dates.

d. COMSEC inspectors will--

(1) Ensure that units manage their COMSEC accounts in accordance with AR 380-5, AR 380-40, and TB 380-41.

(2) Use the COMSEC Audit/Inspection Checklist (app A) to conduct Command COMSEC inspections.

(3) Maintain inspection reports of subordinate unit COMSEC accounts.

e. COMSEC custodians and alternates will comply with the duties and responsibilities specified in AR 380-40 and TB 380-41.

5. COMSEC custodians

a. All COMSEC custodians, alternates and inspectors must have completed the Standardized COMSEC Custodian Course prior to appointment. The USARC Headquarters will consider exceptions on a case-by-case basis.

b. The COMSEC custodian, or at least one of his/her alternates, must be a full-time support (FTS) individual.

6. COMSEC accounts

a. Regional Support Command commanders will establish a COMSEC Material Distribution Support Activity (CMDSA) account at their headquarters. This account will provide COMSEC support to units within their region. Commanders of DRCs and other selected organizations may establish operational accounts to meet their mission requirements.

b. COMSEC accounts will not be established by any RSC subordinates below the brigade or group level.

c. All commands will prepare COMSEC Facility Approval Requests (CAR) for the establishment or relocation of a COMSEC facility/account in accordance with AR 380-19 and DA Pamphlet 25-380-2. Submit CAR(s) through Commander, USARC, ATTN: AFRC-INS, to Director, United States Army Communications Command Security Logistics Activity (USACCSLA). See CAR format at figure 1.

d. A DA Form 2012 (COMSEC Account Data), along with the certificate of training for the COMSEC custodian and alternates, will be included with any request for a new account.

e. The COMSEC custodian will submit requests for new cryptographic key, except STU-III or RCAS, in writing, through command channels to Director, USACCSLA.

7. Physical security

Administer physical security of COMSEC material in accordance with AR 190-16 and AR 380-5.

8. Reporting of COMSEC incidents (RCS exempt, TB 380-41, para 5.25.1)

a. Report COMSEC incidents in accordance with AR 380-19 and DA Pamphlet 25-380-2. The importance of timely reporting of COMSEC incidents cannot be overemphasized or ignored in order to protect our communication secure systems and equipment with a primary objective of maintaining national security at the highest level.

b. The four types of COMSEC incident reports are: initial, amplifying, final, and abbreviated. For detailed instructions/definitions, refer to AR 380-19 and DA Pamphlet 25-380-2.

(1) Prepare each report according to the type of COMSEC security situation involved; i.e., physical, cryptographic, or personnel. For the text and routing information needed for a report, see appendix B.

(2) Base classification of reports on the textual content. For specific guidance in classifying a report, refer to AR 380-5.

(3) The type of material and seriousness involved in the incident will determine the report precedence (if sent by electrical message) and the timeliness assigned. Refer to AR 380-5 for guidance on assigning message precedence or correspondence handling time for reports.

c. To ensure complete protection of COMSEC information, restrict release of information concerning COMSEC incident reports to a need-to-know basis and, in some situations, discuss only by a secure means or within a secure area. For additional information or assistance in the reporting of COMSEC incidents, contact Commander, USARC, ATTN: AFRC-INS.

9. Incident evaluations and investigations

a. ***Evaluations.*** The CONAUTH will conduct evaluations and damage assessments of COMSEC incidents based upon the information provided, taking into consideration the security characteristics of the cryptosystem. The CONAUTH of the material involved will be the prime judge in determining if a compromise of the material did or did not occur. When the evaluation determines that supersession of key/equipment/material is necessary, the CONAUTH of the material must immediately notify all holders of that item and will provide all holders of the material with disposition instructions for the material involved in the incident. For additional guidance, see TB 380-41, paragraphs 5.31 and 5.32.

b. ***Investigations.*** In some situations, commanders may determine that a formal or informal investigation of a COMSEC incident is warranted under the provisions of AR 15-6. COMSEC incidents are normally handled locally by disinterested individuals appointed by the commander to conduct preliminary inquiries. These inquiries will provide or uncover sufficient information to determine whether or not actual compromises have occurred and to recommend measures to prevent recurrence. At the discretion of the commander of the activity, a formal investigation may be ordered and conducted in accordance with AR 15-6. The investigating personnel must be properly cleared for the information involved in the incident.

10. Controlled cryptographic items (CCI)

Manage CCI in accordance with AR 190-51, AR 380-40, TB 380-41, DA Pam 25-16 and DA Pam 25-380-2.

11. Department of the Army Cryptographic Access Program (DACAP)

a. The primary objective of the DACAP is to control personal access to classified cryptographic information by identifying those personnel who would have direct contact with Top Secret Cryptographic information or material. The DACAP applies to--

(1) All U.S. Army military personnel and civilian employees, including those assigned to the Reserve Components, and agents of the Department of the Army, who have access to classified cryptographic information.

(2) COMSEC custodians, alternates, and hand receipt holders.

(3) Producers or developers of cryptographic key or logic.

(4) Personnel who perform administrative and supply functions where cryptographic keying material are generated or stored (only those personnel actually having access to such material).

(5) Personnel in telecommunication centers, secure subscriber terminals, whose duties require keying of cryptographic equipment.

b. The DACAP does not apply to--

(a) Individuals whose duties are to operate (not to key or maintain) systems using cryptographic equipment.

(b) Persons who use a KSD-64A, Cryptographic Ignition Key (CIK) to access the secure features of the STU-III telephone system.

c. The DACAP will be decentralized and managed at the RSC and DRC level. The DACAP applies only to organizations that have Top Secret COMSEC accounts.

d. The Senior Intelligence Officer (SIO) or Security Manager at each organization will--

(1) Provide program oversight.

(2) Implement the DACAP for those activities that have Top Secret COMSEC accounts.

(3) Identify an individual at each activity to serve as the point of contact (POC) with the U.S. Army Intelligence and Security Command (INSCOM) polygraph elements. The POC will be responsible for coordinating the details of all required polygraph examinations. The POC will also provide INSCOM with the number of participants to be examined (that number will be equal to 25 percent of the total number of program participants). Forward required information to Commander, 902d Military Intelligence Technical (MIT) Battalion (CounterIntelligence). ATTN: IAGPA-A-OP, Fort George G. Meade, MD 20755-5955. Preferred method of transmission is unsecure facsimile. Provide an information copy to Commander, USARC, ATTN: AFRC-INS.

(4) Changes and updates to the initial input for the DACAP will be the sole responsibility of the designated POC of the organization.

(5) The POC will--

(a) Identify those personnel who require cryptographic access and ensure they receive the cryptographic access briefing and sign a USARC Form 65-R (Cryptographic Access Authorization and Termination) (see app C). The POC will retain certification within the activity files as proof of completion.

(b) Randomly select the appropriate number of individuals for polygraph examination when notified by the INSCOM polygraph examination representative.

(c) Ensure that individuals who have been selected for polygraph examination are available at the time and place so designated for the examination.

(d) Deny cryptographic access to, or withdraw cryptographic access from, those individuals who fail to comply with any of the criteria outlined in AR 380-40, paragraphs 1-4g(6)-(8) and h(5)-(8).

(6) A representative from the 902d MIT Battalion will contact the organization POC representative to pass DACAP scheduling information for examinations. The POC will in turn schedule unit personnel for polygraph examinations and forward the names of the personnel to the 902d MIT Battalion.

e. Each organization must ensure full compliance in meeting the DACAP program criteria.

f. Direct any questions regarding the DACAP to Commander, USARC, ATTN: AFRC-INS.

CLASSIFICATION
(AT A MINIMUM FOUO)

LETTERHEAD

AFRC-XXX (380-40a)

MEMORANDUM THRU Commander, U.S. Army Reserve Command, ATTN:
AFRC-INS, 3800 North Camp Creek Parkway, SW,
Atlanta, GA 30331-5099

FOR Director, United States Army Communications-Electronics
Command, Communications Security Logistics Activity, ATTN:
SELCL-KPD-AU, Fort Huachuca, AZ 85613-7090

SUBJECT: COMSEC Facility Approval Request (CAR)

1. References:

a. AR-380-40 (Department of the Army Policy for Safeguarding and Controlling COMSEC Information).

b. TB 380-41 (Procedures for Safeguarding, Accounting and Supply of COMSEC Material).

c. AR 380-5 (Department of the Army Information Security Program).

2. This command has a requirement to (establish) (alter) (relocate) a COMSEC facility. ***[Complete as appropriate.]***

a. The following information is submitted IAW paragraph 2.1.2, TB 380-41, Oct 94 (or latest update/revision).

(1) Requesting Unit: ***[Complete mailing address and UIC.]***

(2) Telephone Number: ***[DSN and Commericial number if available.]***

(3) COMSEC Account Number: ***[If for new account, ENTER TBA (to be assigned).]***

(4) Facility Location: ***[Enter complete address, to include, building, room, floor numbers. (Must be complete for courier address.)]***

(5) Type of Facility: ***[Fixed or Mobile (in most cases fixed).]***

(6) Purpose of Facility: ***[Storage, Operation, Admin, etc.]***

(7) System/Equipment: ***[E.g., TSEC/KY-57, TSEC/KG-30. (Use Short title of "System" O/H or AUTH, DO NOT LIST COMPONENTS.)]***

(8) Highest classification of material to be held: ***[TOP SECRET, SECRET, etc. (EQUIPMENT OR KEY).]***

(9) Physical Security: ***[Describe facility construction; e.g., Cement block walls, poured concrete floor, lightweight concrete ceiling and two solid wood doors. Describe other factors; e.g., security locks, containers, barred windows. Give actual physical measurements of facility; e.g., doors, windows, thickness of walls, ceiling, floor (if not on a slab). SUGGEST YOU PROVIDE A LIMITED SKETCH OF THE FACILITY. (IF MULTI-LEVELS, SHOW ALL LEVELS AND SPECIFY EXACT LQCATION QF YOUR FACILITY.)]***

(10) Protection of COMSEC material: ***[Explain how material is stored within the facility in accordance with AR 190-51, AR 380-5, and DA Pamphlet 380-2. Store classified equipment and keying material in a GSA-approved security container. Store TOP SECRET key under Two-Person Integrity (TPI) procedures, employing two different container combination locks, with no one person having access to both container combinations. One of the lock combinations is built in the container. The second combination is affixed to the insert container located within the two-drawer GSA approved safe. All persons having access to the TPI container(s) will have a TOP SECRET clearance. Explain how all COMSEC material is protected during work and non-duty hours and describe any supplemental security measures that will be in effect.]***

b. Affirmation: Applicable standards can be met for the operation, storage, and destruction of COMSEC material, as outlined in TB 380-41. ***[This is a standard statement.]***

3. For additional information, contact ***[(Name), DSN/Commercial telephone number(s)].***

FOR THE COMMANDER ***[If appropriate]***

SIGNATURE BLOCK OF COMMANDER
(or Authorized Rep)

Figure 1. COMSEC Facility Approval Request (CAR) format

Appendix A
COMSEC Audit/Inspection Checklist

The following checklist contains questions covering those vital areas the COMSEC auditor/inspector will examine during the audit/COMSEC facility inspection.

A-1. Is a Restricted Area Visitor Register (DA Form 1999-R) being properly maintained by the account *(AR 380-40, para 4-6c and TB 380-41, para 5.2c)*, and is a Privacy Act Statement being displayed near the Visitors Register? *(TB 380-41, para 5.2d)* Is an access list being maintained? *(AR 380-40, para 4-6)*

A-2. Has the COMSEC custodian satisfactorily completed the TRADOC-approved Standardized COMSEC Custodian Course prior to their appointment or is he/she scheduled to attend in the near future? *(AR 380-40, para 2-lb and TB 380-41, para 2.7b)* When?

A-3. Does the reference library used by COMSEC personnel contain copies of AR 380-40, TB 380-41? *(AR 380-40, para 1.2)*

A-4. Is the COMSEC account custodian maintaining a copy of the Cryptofacility Approval and the initial request for that approval? *(AR 380-40, para's 4-3 and 4-4, and TB 380-41, para 2-1)* Is the approval current? Have any changes occurred, such as relocation of the facility,changes/modifications made to the facility, room number, other changes?

A-5. Is the COMSEC Account Data (DA Form 2012) prepared correctly? *(TB 380-41, para 2-12)* Is it up-to-date and are the clearances of the listed personnel at least equal to the Cryptofacility approval?

A-6. Is a copy of the latest USACCSLA audit/inspection and Command inspection on file *(AR 380-40, para 6-2b and TB 380-41, para 4.6),* and were all discrepancies discovered during the USACCSLA audit/inspection and command inspection reconciled? *(AR 380-40, para 6-2c)*

A-7. Is the COMSEC material being protected/stored properly? *(AR 380-40, para 2-15, and TB 380-41, para 5.8)* Is Top Secret COMSEC material being protected/stored properly? *(AR 380-40, para's 2-17 and 2-18 and TB 380-41, para 5.8.1a)*

A-8. Have the combinations to security containers been changed? *(AR 380-5, para 5-104 and TB 380-41, para 5.1.4h)* Are Standard Forms 700/701/702 being maintained by the account custodian? *(AR 380-5, para 5-104 and TB 380-41, para 5.4)*

A-9. Is a COMSEC Account Daily Shift Inventory (DA Form 2653-R) being maintained by the account custodian? *(TB 380-41, para 4.15c)*

A-10. Is the COMSEC custodian aware of the procedures for inspecting keying material for signs of tampering upon initial receipt, during inventory and prior to each use? *(AR 380-40, para 2-18h and TB 380-41, para 4.7)*

A-11. Is a physical inventory taken of all COMSEC material located in the account? *(TB 380-41, para 4.16)* Are there any superseded key/publications (ARKAG-1) on hand that should have been destroyed? *(TB 380-41, para 4.22)*

A-12. Does the COMSEC account still maintain accountability of Controlled Cryptographic Items (CCI)? *(TB 380-41, para 3.2.1b)*

A-13. Is the COMSEC custodian maintaining keying material in the COMSEC account for which no requirement exists? *(TB 380-41, para 3.9)* Does he/she understand the intended use of any keying material currently in possession? *(TB 380-41, para 3.4)* In terms of production, distribution, storage, and destruction cost, could their operational key be placed in a contingency status? *(TB 380-41, para 3-4)*

A-14. Does the COMSEC custodian know who the controlling authorities are for all key material maintained in the account? *(TB 380-41, para 3.4)*

A-15. Has a complete page check of all accountable COMSEC publications been performed? *(TB 380-41, para* 4.7. 6*)* Have all amendments been posted and residue destroyed? *(TB 380-41, para 4.18)*

A-16. Are the COMSEC account files prepared IAW the Modern Army Recordkeeping System (MARKS) and are old files and publications being disposed of properly? *(AR 25-400-2 & TB 380-41, para 4.6)*

A-17. Was all material on hand receipt physically inventoried for the audit and is a hand receipt holder's briefing statement on file within the account? *(AR 380-40, para 2-11 & TB 380-41, para 4.14 & 4.19.2d)*

A-18. Are Item Register (IR) cards being prepared/maintained and has all material received by the COMSEC custodian been recorded on item register cards? *(TB 380-41, para 4.10)*

A-19. Are the COMSEC Material Reports (SFs 153) being prepared correctly? *(TB 380-41, para 4.12)*

A-20. Are Consolidated Destruction Reports being prepared correctly? *(TB 380-41, para 4.22.4b)*

A-21. Are the COMSEC Material Voucher Control Registers (DA Form 4669-R), Outgoing & Local, being properly maintained? (Example: 0001-4999 for outgoing vouchers reportable to the ACCOR and 5000-9999 for Local vouchers) *(TB 380-41, para 4.)*

A-22. Is the destruction of COMSEC material being properly documented and reported? *(TB 380-41, para 4.11 & 4.22)*

A-23. Are the destruction methods (burning, shredding, pulverizing, etc.) being used by the COMSEC custodian? *(TB 380-41, para 4.22)*

A-24. Is the COMSEC custodian signing reports received/completed by the alternate custodian during the custodian's absence? *(TB 380-41, para 2.8a(2) & 4.16.1d(4))*

A-25. Are the Certification/Correction pages to Semi-Annual Inventory Reports (SAIR) and Change of Custodian Inventory Reports (CCIR) being prepared? *(TB 380-41, para 4.16)*

A-26. Is all ALC 3 material inventoried at least semiannually (SAIR) and upon change of COMSEC custodians? *(TB 380-41, para 4.16.5)*

A-27. Is all ALC 4 material inventoried locally inventoried annually and upon change of COMSEC custodians? *(TB 380-41, para 4.16.5)*

A-28. Is a DD Form 1435 (COMSEC Maintenance Training & Experience Record) prepared for all personnel engaged in the installation, maintenance, or repair of COMSEC equipment? *(AR 25-12, chapter 4)*

A-29. Does the COMSEC account custodian maintain Standing Operating Procedures (SOP)? *(TB 380-41, para 2.2.a)*

A-30. Is an Emergency Plan being maintained and are quarterly drills (dry runs) being conducted? *(AR 380-40, para 3-4 and TB 380-41, para 5.18)*

A-31. Is the account's Defense Courier Service (DCS) Form 10 valid? *(AR 380-40 and TB 38041)*

A-32. Has a Department of the Army Cryptographic Access Program (DACAP) been established and are personnel enrolled in the program? (Ask to see the cryptographic access certification) *(AR 380-40, chap 8)*

A-33. Is there a completed copy of the last Management Control Evaluation (DA Form 11-2-R) filed within the COMSEC account? *(AR 380-40, app D)*

A-34. Are there Telephone Monitoring Decals (DD Form 2056) placed on the front of each common telephone within the inspected activity? *(AR 380-53)*

A-35. For Secure Telephone Units (STU), has the DD Form 2056 been applied to the instrument and the wording "DO NOT DISCUSS CLASSIFIED INFORMATION" on the form been removed or obliterated? *(AR 380-53)*

A-36. Do all computer systems have a log-in screen with the following statement: "DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON NON-SECURE TELECOMMUNICATIONS SYSTEMS. OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS, INCLUDING THIS COMPUTER SYSTEM ARE SUBJECT TO TELECOMMUNICATION SECURITY MONITORING AT ALL TIMES. USE OF THIS COMPUTER SYSTEM CONSTITUTES CONSENT TO TELECOMMUNICATIONS SECURITY MONITORING"? *(AR 380-53)*

Appendix B
Incident Reports

B-1. Routing of reports

COMSEC incident reports are official command correspondence which are to be submitted by or for the commander. Activities/units submitting incident reports should use direct channels to ensure report is received within the required time frame as specified in TB 380-41, chapter 5.

B-2. Report preparation

Prepare each report according to the type of COMSEC security situation involved; i.e., physical, cryptographic, or personnel. These types of incidents and the information required for each type of report is described below.

a. **Physical incident.** This type of incident involves the loss, theft, loss of control, capture, recovery by salvage, tampering, or unauthorized viewing, access, or photographing of classified COMSEC material. The incident report must contain the following information:

(1) Account Number. Enter account number involved.

(2) Material Identification. Reflect complete identification of material involved:

(a) Short Title (include edition designator).

(b) System Indicator, if applicable.

(c) Accounting/Serial Number(s) of accounting legend code (ALC) 1 and 3 material.

(3) Keyed or Unkeyed. If equipment or components were involved, indicate which status.

(4) Incident Description. Describe the incident, including date and time of discovery, and answers to the questions WHO, WHAT, WHEN, WHERE, WHY, and HOW?

(5) Compromise. Estimate the probability of possible compromise; e.g., compromise CERTAIN, PROBABLE, IMPROBABLE, POSSIBLE, IMPOSSIBLE.

(6) Key. If key is involved, identify the CONAUTH.

(7) Missing Material. When material is missing, include the following information:

(a) Date and Location: List the date, location, and circumstance of the last known sighting.

(b) Cause of Loss. List all available information pertaining to the cause of loss.

(c) Actions Taken. List all actions being taken to locate the material.

(d) Unauthorized Access. Indicate the possibility of access by unauthorized persons.

(e) Disposal Method Used. Indicate the disposal method used for classified and unclassified waste.

(8) Temporary Loss. In the event material is temporarily lost or otherwise out of proper channels, include the following information:

(a) Time and Circumstances. Indicate the exact period of time and under what circumstances the material was discovered to be out of proper channels.

(b) Action. Indicate the action which caused the material to be returned to proper channels.

(c) Clearance Status. Indicate the clearance status of persons having authorized access to the material.

(d) Surreptitious Access. Indicate the possibility of surreptitious access by unauthorized persons.

(9) Damaged Package. When a package is damaged or shows evidence of possible tampering, report circumstances that are involved. See TB 380-4l, paragraph 5.28.4.

(10) Unauthorized Access. When an unauthorized person(s) had access to classified COMSEC material or information, include in your report the following:

(a) Identity of Person(s). Indicate the identity of each person and their clearance status.

(b) Accompanied by Cleared Personnel. Indicate whether the unauthorized person(s) was (were) accompanied by cleared personnel.

(c) Time. Indicate the length of time the person(s) had access.

(11) Material Left Unprotected. Unprotected material includes material in safes, containers, rooms or vaults which have been left open or unlocked, or were discovered to have malfunctioning locking devices. See TB 380-41, paragraph 5.28.6.

b. **Personnel incident.**

(1) This type of incident is when a person having access to classified COMSEC information is suspected of ESPIONAGE, DEFECTION, SUBVERSION, or SABOTAGE; is declared AWOL; is CAPTURED; or has had his/her CLEARANCE REVOKED for cause: Include the following information in the Personnel Incident Report:

(a) COMSEC account number(s).

(b) Individual's full name, rank/grade and SSN.

(c) Date and circumstances of the incident.

(d) Results of inventories and preliminary local investigations.

(e) Results of Counter-Intelligence interviews, inter-relations, and investigations.

(f) List of missing COMSEC material or lists of all classified material to which the person had access at the time of the incident.

(g) Provide a statement of the individual's background in COMSEC and his/her knowledge of cryptoprinciples.

(2) Final Reports. All personnel incidents require final reports. *[**NOTE:** Initial or subsequent reports may serve as the final report by adding a statement as follows: The inquiry/interview/interrogation showed no evidence of possible compromise of classified COMSEC information. This is a Final Report.]*

c. **Cryptographic incident.** Cryptographic incidents associated with each cryptosystem are identified in the operating and maintenance instructional manuals (KAO/KAM). Include the following information in the incident report:

(1) Equipment Malfunctions.

(2) Identify the equipment or components involved.

(3) Describe how, and under what conditions, the equipment was being used at the time of the incident.

(4) Identify the symptoms of the malfunction. Indicate the possibility that the malfunction was deliberately caused, if applicable.

(5) In the event equipment was used to send operational traffic, identify the TRAFFIC and the SHORT TITLE of any key involved.

(6) Unauthorized Cryptoperiod Extension. When the incident involves an unauthorized extension of a prescribed cryptoperiod, include the following information in the cryptographic incident report:

(7) Describe the associated communications activity (e.g., on-line/off-line, simplex, half duplex, transmit only/receive only).

(8) Indicate the operating mode of the COMSEC equipment (e.g., message indicator, traffic flow security) and the operating speed.

(9) Report the number of messages sent or received, the number of messages received garbled, and the general type of traffic involved (e.g., COMINT, intelligence, formatted, data, speech, teletypewriter).

B-3. Electrical message addresses

Below are the specific electrical message address elements for each category of incident. *[**NOTE:** Addressee elements should be rechecked with local Telecommunication Center for accuracy. For activities not having electrical message capability, the incident report must be submitted in memorandum format through command channels. If the report is classified, proper procedures must be applied IAW AR 380-5 for packaging and method of mailing through postal channels.]*

a. **Physicial incident.**

(1) Cryptographic Key (User Level)

ACTION ADDRESSEE

* CONTROLLING AUTHORITY(s) of the Short Title(s) involved
* CDR902DMIGP FT GEORGE G MEADE MD//IAGPA-CIMO//

INFORMATION ADDRESSEE

* CDRINSCOM FT BELVOIR VA//IAOPS-HU/CI//
* DIRNSA FT GEORGE G MEADE MD//V51A//
* DIRUSACCSLA FT HUACHUCA AZ//SELCL-KPD-OR//
* CDRFORSCOM FT MCPHERSON GA//AFIN-CIS//
* CDRUSARC FT MCPHERSON GA//AFRC-IN//
* OTHER COMMAND CHANNELS AS APPROPRIATE

(2) Cryptographic Key in Distribution Channels

ACTION ADDRESSEE

* CDR902DMIGP FT GEORGE G MEADE MD//IAGPA-CIMO//
* DIRNSA FT GEORGE G MEADE MD//V5lA//

INFORMATION ADDRESSEE

* CONTROLLING AUTHORITY OF KEYING MATERIAL
* DIRUSACCSLA FT HUACHUCA AZ//SELCL-KPD-OR//
* CDRINSCOM FT BELVOIR VA//IAOPS-HU/CI//
* CDRFORSCOM FT MCPHERSON GA//AFIN-CIS//
* CDRUSARC FT MCPHERSON GA//AFRC-IN//
* OTHER COMMAND CHANNELS AS APPROPRIATE

b. Cryptographic incident

ACTION ADDRESSEE

* DIRNSA FT GEORGE G MEADE MD//V51A//
* CDR902DMIGP FT GEORGE G MEADE MD//IAGPA-CIMO//

INFORMATION ADDRESSEE

* CDRINSCOM FT BELVOIR VA//IAOPS-HU/CI//
* CDRFORSCOM FT MCPHERSON GA//AFIN-CIS//
* CDRUSARC FT MCPHERSON GA//AFRC-IN//
* OTHER COMMAND CHANNELS AS APPROPRIATE

NOTES:
1. For effective or near future key, assign an immediate message precedence to all action addressees.
2. For superseded, reserve, and contingency key, assign priority precedence to all action addressees.

c. Personnel incident

ACTION ADDRESSEE

* CDR902DMIGP FT GEORGE G MEADE MD//IAGPA-CIMO//

INFORMATION ADDRESSEE

* CDRINSCOM FT BELVOIR VA//IAOPS-HU/CI//
* DIRNSA FT GEORGE G MEADE MD//V51A//
* CDRFORSCOM FT MCPHERSON GA//AFIN-CIS//
* CDRUSARC FT MCPHERSON GA//AFRC-IN//
* ALL OTHER COMMAND CHANNELS AS APPROPRIATE

NOTES:
1. For address elements when using standard memorandum format, use plain address elements normally applied to formal memorandum correspondence.
2. See paragraph 8,this regulation, and paragraphs B-1 and B-2, above, for additional guidance and detailed information on submitting incident reports.

Appendix C
DACAP Access Briefing and Authorization/Termination

C-1. Cryptographic Access Briefing
The security manager and/or the POC will use the following briefing ***verbatim*** to indoctrinate individuals for cryptographic access.

CRYPTOGRAPHIC ACCESS BRIEFING

You have been selected to perform duties that will require access to classified cryptographic information. It is essential that you be made aware of certain facts relevant to the protection of this information before access is granted. You must know the reason why special safeguards are required to protect classified cryptographic information. You must understand the directives which require these safeguards and the penalties you will incur for the unauthorized disclosure, unauthorized retention, or negligent handling of classified cryptographic information. Failure to properly safeguard this information could cause serious or exceptionally grave damage, or irreparable injury, to the national security of the United States or could be used to advantage by a foreign nation.

Classified cryptographic information is especially sensitive because it is used to protect other classified information. Any particular piece of cryptographic keying material and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system may be compromised. The safeguards placed on classified cryptographic information are a necessary component of Government programs to ensure that our Nation's vital secrets are not compromised.

Because access to classified cryptographic information is granted on a strict need-to-know basis, you will be given access to only that cryptographic information necessary in the performance of your duties. You are required to become familiar with AR 380-40 as well as those publications referenced therein.

Especially important to the protection of classified cryptographic information is the timely reporting of any known or suspected compromise of this information. If a cryptographic system is compromised, but the compromise is not reported, the continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary's advantage gained through the compromise of the information.

As a condition of access to classified cryptographic information, you must acknowledge that you may be subject to counterintelligence scope polygraph examination. This examination will be administered in accordance with DOD DIR 5210.48 and applicable law. The relevant questions in this polygraph examination will only encompass questions concerning espionage, sabotage, or questions relating to unauthorized disclosure of classified information or unreported foreign contacts. If you do not, at this time, wish to sign such an acknowledgement as a part of executing a cryptographic access certification and termination memorandum, this briefing will be terminated at this point and the briefing administrator will so annotate the memorandum. Such refusal will not be cause for adverse action but will result in your being denied access to classified cryptographic information.

You should know that intelligence services of some foreign governments prize the acquisition of classified cryptographic information. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion to divulge classified cryptographic information. You should be alert to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, classified cryptographic information and thus avoid highlighting yourself to those who would seek the information you possess. Any attempt, either through friendship or coercion, to solicit your knowledge regarding classified cryptographic information must be reported immediately to (insert the name and phone number of the supporting counterintelligence unit).

In view of the risks noted above, if unofficial foreign travel becomes necessary, it is essential that you notify (insert appropriate security office) and receive the appropriate travel briefing.

Finally, you must know that, should you willfully or negligently disclose to any unauthorized persons any of the classified cryptographic information to which you will have access, you may be subject to administrative and civil sanctions, including adverse personnel action, as well as criminal sanctions under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States, as appropriate.

C-2. USARC Form 65-R (Cryptographic Access Authorization and Termination)

a. The USARC Form 65-R is a two-part form. The security manager or POC will--

(1) Ensure individual being granted access to classified cryptographic information reads, completes, and signs Section I before granting that individual access to U.S. classified cryptographic information.

(2) Ensure individual having access to classified cryptographic information withdrawn reads, completes, and signs Section II when the individual no longer requires such access.

(3) Complete and sign Section I and Section II as the "administering official".

b. Until cryptographic access is terminated and Section II of the USARC Form 65-R is completed, the cryptographic access granting official shall maintain the form in a legal file system which will permit expeditious retrieval. Further retention of the form will be as specified in AR 25-400-2 for file number 380-5a.

c. A blank copy of USARC Form 65-R is at the back of this regulation for reproduction purposes.

Glossary

ALC ..... accounting legend code

CAR..... Communication Facility Approval Request
CCI ..... controlled cryptographic item
CER ..... Cryptographic Evaluation Report
CIK ..... Cryptographic Ignition Key
CMDSA ..... Communication Security Material Direct Support Activity
COMSEC ..... communications security
CONAUTH ..... controlling authority

DACAP..... Department of the Army Cryptographic Access Program
DRC..... direct reporting command

INSCOM..... Intelligence and Security Command

KAM..... Cryptographic Operational Maintenance Manual
KAO ..... Cryptographic Operational Operating Manual

RCAS..... Reserve Component Automation System
RSC ..... Regional Support Command

SCCC..... Standard COMSEC Custodian Course
SIO ..... Senior Intelligence Officer
STU-III ..... Secure Telephone Unit, Third Generation

TPC..... two-person control
TPI..... two-person integrity

USACCSLA..... United States Army Communications Command Security Logistics Activity