UNC/CFC Reg 380-1
유엔사/연합사 규정 380-1

HEADQUARTERS

UNITED NATIONS COMMAND/ROK-US COMBINED FORCE COMMAND
유엔군사령부/한미연합군사령부
APO AP 96205

REGULATION
규정

1APR 1998
1998.4.1

NUMBER 380-1
번호 380-1

SECURITY
보안

UNC/CFC INFORMATION SECURITY PROGRAM
유엔사/연합사 정보보안규정

HEADQUARTERS
UNITED NATIONS COMMAND/ROK-U.S. COMBINED FORCES COMMAND
APO AP 96205

REGULATION
NUMBER 380-1 **1 April 1998**

UNC/CFC INFORMATION SECURITY PROGRAM

The word "he" when used in this regulation represents both genders, unless otherwise specifically stated. Local supplementation of this regulation is prohibited except upon approval of the Assistance Chief of Staff, C2.

*This regulation supersedes UNC/CFC Regulation 380-1, dated 10 Feb 92.

CHAPTER 1

GENERAL PROVISIONS

1-1. PURPOSE:

This regulation establishes an Information and Personnel Security Program for Headquarters, United Nations Command (UNC), ROK/U.S. Combined Forces Command (CFC) and other ROK/U.S. combined activities.

1-2. SCOPE:

The procedures prescribed herein will maximize the safeguarding and control of defense information bilaterally created within this combined environment. Such information is hereby designated as ROKUS information. ROK-only or U.S. only defense information created or maintained within the combined area will be safeguarded in accordance with respective national regulations or directives.

1-3. RESPONSIBILITIES:

a. The ACofS, C2 has primary staff responsibility for all matters pertaining to combined information and personnel security.

b. The Chief, Security Branch, ACofS, C2, is responsible for planning, developing and implementing the command combined information and personnel security policy; identifying systemic problems and devising solutions to resolve complex and sensitive security issues; assessing the adequacy of command initiatives; providing training and education and conducting oversight inspections and staff assistance visits.

c. UNC/CFC Headquarters staff principals and ROK/U.S. combined activity commanders will appoint, in writing:

(1) A Security Manager (SM), 0-3 or above, and an alternate, E-7 or above. If the SM is a ROK service member, the alternate must be a U.S. service member and vice/versa. Staff/activity SMs will be responsible for the administration of an effective information and personnel security program within their areas of responsibility. The SM will:

(a) Publish bilingual Standing Operating Procedures (SOP) for his activity to govern the creation, classification, declassification, disposition and safeguarding of classified material.

(b) Advise and represent his appointing authority on matters pertaining to information and personnel security.

(c) Establish procedures for ensuring that all personnel who are to handle classified material are appropriately cleared and trained on their duties and responsibilities for safeguarding such material. The clearance status of each individual, including UNC, ROK and U.S., will be recorded and accessible for verification purposes. The SM or alternate shall personally ensure all persons are trained prior to their initial access to classified material. This training shall be documented and retained in SM files until the individual has departed the command. Security training is an annual requirement.

(d) Advise and assist officials on individual classification decisions and on development of appropriate classification guidance (See U.S. DoD 5200.1H), ensuring preparation and issue of classification guidance for assigned plans, programs and projects.

(e) Carry out a continuing declassification and destruction program. Ensure that classified holdings are reviewed at least annually and that those no longer required are destroyed.

(f) Assist and advise the appointing authority in matters pertaining to the enforcement of information, personnel and appropriate security program regulations.

(g) Be the single point of contact within the staff section to coordinate and act on personnel and information security problems.

(h) Be senior in rank to the Top Secret-ROKUS Control Officer (TSRCO)

(i) Supervise or conduct announced and unannounced security inspections and spot checks to determine compliance with this regulation and other security directives. The security inspections will consist of at least two inspections annually, one unannounced inspection conducted after-duty hours, and one announced inspection conducted during duty-hours. In addition, unannounced spot checks will be conducted throughout the year. Records of security inspections and spot checks will be maintained for a period of at least one calendar year or until the completion of the next Command Security Inspection or Staff Assistance Visit.

(2) A TSRCO and alternate, E-7 or above, will be appointed when the staff section receives, produces, processes, handles, monitors,

or disseminates Top Secret-ROKUS (TS-R) material. TSRCOs will:

(a) Be responsible for safeguarding and accounting for all TS-R material in the custody of the staff section or agency.

(b) Have physical custody and complete accountability of all TS-R documents/material charged to his account.

(c) Receive and enter on his account all incoming TS-R documents/material.

(d) Sign out TS-R documents/material to properly cleared members of his staff section on temporary receipts or permanently transfer the documents outside of his account.

(e) Conduct required annual inventory and account to the HQ CFC TSRCO for all TS-R documents/material charged to his account.

(f) Destroy, and certify in writing the destruction of TS-R documents/material no longer required.

(g) Obtain the approval of the originator and certify such approval in writing, when reproduction of TS-R material is required.

(h) Ensure reproduced copies of TS-R documents are clearly marked and brought under proper control and accountability.

1-4. DEFINITIONS:

a. Classification: The determination that official information requires, in the interest of mutual security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

b. Classified Information: Official information which has been determined to require, in the interest of mutual security, protection against unauthorized disclosure and which has been so designated.

c. Classifier: An individual who:

(1) Determines that official information, not known by him to be already classified, currently requires, in the interest of mutual

security, a specific degree of protection against unauthorized disclosure and having the authority to do so, designates that official information as TOP SECRET-ROKUS, SECRET ROKUS, or CONFIDENTIAL-ROKUS under the Original Classification Authority.

(2) Determines that official information is in substance the same as information known by him to be already classified TOP SECRET-ROKUS, SECRET-ROKUS, or CONFIDENTIAL-ROKUS and designates it accordingly.

d. Compromise: The known or suspected disclosure of classified information or material to an unauthorized person.

e. Custodian: An individual who has possession of or is otherwise responsible for safeguarding and accounting of classified information.

f. Declassification: The determination that classified information no longer requires, in the interest of mutual security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

g. Document: Any record of information, regardless of its physical form or characteristics, including, without limitation, written or printed material; data processing media, charts, drawings, engravings, sketches, working notes and papers; reproduction of such things by any means or process; and sound voice, or electronic recordings in any form; plus photographs videotapes, films, and typewriter ribbons.

h. Downgrade: The determination that classified information requires, in the interest of mutual security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree.

i. Information: Knowledge which can be communicated by any means.

j. Material: Any document, product or substance on or in which information may be recorded or embodied.

k. ROKUS: Defense information bilaterally created within a combined ROK and U.S. environment. May be classified or unclassified.

l. Security Container: A safe or security cabinet meeting specific structural criteria for the storage of classified material, where the material may be stored outside of an approved security vault.

m. Security Vault: An area meeting specific structural criteria approved for the storage of classified material, where the material may be stored openly or in non-approved containers.

n. Security Violation: A violation of security rules, regulations and/or practices which may or may not result in a compromise.

1-5. POLICIES:

a. Classification, when required, will be retained for a minimum length of time, considering the degree of sensitivity and effect of compromise.

b. Unnecessary classification (over-classification) is prohibited.

c. Possible compromise and security violations will be telephonically reported to the C2, Security Branch within 24 hours of discovery. A preliminary investigation will be conducted within 10 days in accordance with paragraph 7-4.

1-6. ADMINISTRATIVE AND JUDICIAL ACTION:

The UNC, ROK and U.S. Governments will take appropriate administrative and/or judicial action in accordance with applicable national law for violations of the regulation.

Chapter 2

CLASSIFICATION

2-1. CLASSIFICATION CRITERIA, POLICIES, AND CONSIDERATIONS:

See Appendix B.

2-2. SECURITY CLASSIFICATION CATEGORIES:

a. Official Information or material which requires protection against unauthorized disclosure in the interest of mutual security will be classified in one of three categories, "TOP SECRET-ROKUS, SECRET-ROKUS, OR CONFIDENTIAL-ROKUS", depending upon the degree of its significance to mutual security. No other categories will be utilized to protect official information.

(1) TOP SECRET-ROKUS refers to that mutual security information or material which requires the highest degree of protection. The test for assigning "TOP SECRET-ROKUS" classification will be whether its unauthorized disclosure could: reasonably be expected to cause exceptionally grave damage to mutual security; such as leading to a disruption of diplomatic relations or the outbreak of war; threatening strategic military defensive plans; jeopardizing the U.S. or ROK military intelligence capabilities; or compromising the development of essential national defense technologies. This classification will be used with the utmost restraint. U.S. information classified Top Secret may not be used for input to Top Secret-ROKUS information.

(2) SECRET-ROKUS refers to that mutual security information or material which requires a substantial degree of protection. The test and evaluation for assigning "SECRET-ROKUS" classification will be whether its unauthorized disclosure could reasonably be expected to cause serious damage to mutual security.

(3) CONFIDENTIAL-ROKUS refers to that information or material which requires protection. The test and evaluation for assigning "CONFIDENTIAL-ROKUS" classification will be whether its unauthorized disclosure could reasonably be expected to cause identifiable damage to mutual security.

2-3. AUTHORITY TO CLASSIFY:

a. "Original Classification Authority" is authority to make a decision that official information requires, in the interest of mutual security, a specific degree of protection against unauthorized disclosure. This authority is restricted solely to those officials specifically

designated. It is vested in the incumbent of the designated position or in the individual designated in writing by the incumbent to act in his absence. The exercise of this authority is the responsibility of these officials and may not be delegated by them or used by anyone acting for them or in their names. It is limited to classification only at the level indicated or a lower classification. Designation of this authority will be limited to those officials whose duties and responsibilities involve the origination and evaluation of information warranting classification at the level stated in the designation. The CINC, CFC is the original TOP SECRET-ROKUS classification authority. (See appendix C.)

b. "Derivative classification authority" is vested in all persons who possesses a valid security clearance. They may classify documents based on the classification of source document(s) and/or verbal guidance from an original classification authority. They will assign downgrading and declassification instructions accordingly. "Derivative classification authority" may be exercised by all personnel with appropriate security clearance and need-to-know.

2-4. RECIPIENT OF CLASSIFIED INFORMATION OR MATERIAL:

If the recipient of classified information or material believes it should not be classified or that current security considerations justify a change in the assigned classification, he should make such changes if he is a higher official in the same chain of command. If not, he will promptly submit the matter to the appropriate classifier with his recommendation and reasons therefore. Pending final determination, the information or material will be safeguarded by the higher classification until the classification is changed or otherwise verified. The responsible classifying authority will act on such recommendation promptly.

2-5. IDENTIFICATION OF CLASSIFIER:

Information or material classified under this regulation will indicate on its face, in the case of documents, or by notice or other means, in the case of material, the identify of the classifier or source document. Such identification will be shown in the "Classified by" line for original classification and "Derived by" line for derivative classification respectively.

2-6. COMPILATION OF INFORMATION:

Compilations of unclassified information is not classified, unless such compilation provides an added factor which warrants classification.

Chapter 3

DECLASSIFICATION AND REGRADING

3-1 DECLASSIFICATION INSTRUCTIONS:

When classifying a document a determination must be made of length of classification. General rule is that classified material shall be downgraded, declassified, or destroyed when there are no grounds for continued classification.

a. Automatic declassification of classified information occurs after 25 years unless the information was classified under one of seven exemption categories as listed in Appendix B.

b. Downgrading occurs when the classified material no longer require the higher level of classification.

c. Declassification and downgrading require the Original Classifier's permission.

Chapter 4

MARKINGS

4-1. CLASSIFICATION MARKINGS ON DOCUMENTS:

a. The overall classification of a document, whether or not permanently bound, or any copy of reproduction thereof, will be conspicuously marked or stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page of a document will be conspicuously marked or stamped at the top and bottom with the highest classification of information appearing thereon, including the designation "UNCLASSIFIED" when appropriate. "ROKUS" will appear with classification markings.

(1) Rubber stamps or computer generated markings will be used.

(2) Document markings will be in black ink, except on message forms (DD Form 173).

b. Each section, part, paragraph, subparagraph, or similar portion of a classified document will be marked to show the level of classification of the information contained in or revealed by it, or that it is unclassified. Portions of documents will be marked in a manner that eliminates doubt as to which portions contain or reveal classified information. Classification levels of portions of a document will be shown by the appropriate classification symbol placed immediately following the portion letter or number, or in the absence of letters of numbers, immediately before the beginning of the portion. In marking sections, parts, paragraphs, subparagraphs, or similar portions the parenthetical symbols "TS-R" for TOP-SECRET-ROKUS, "S-R" for SECRET-ROKUS, "C-R" for CONFIDENTIAL-ROKUS, and "U-R" for UNCLASSIFIED-ROKUS will be used. To illustrate the foregoing, if a lead-in paragraph is unclassified and a subparagraph is SECRET-ROKUS, the markings will be:

(1) (U-R) This is the unclassified lead-in paragraph.

(2) (S-R) This is the classified subparagraph.

c. Subjects or titles, of classified documents will be marked with the appropriate symbol, "TS-R", "S-R", "C-R", or "U-R", immediately following and to the right of the subject or title. Subjects or title of documents will be unclassified, if possible. If it becomes necessary to classify the subject or title the appropriate symbol, "TS-R", "S-R", "C-R" will be placed to the left of the subject or title. By applying this

action, the handler of the document will be alerted to the fact that not only are the contents of the documents classified but the title above cannot be released to unauthorized persons.

d. Files, folders, or groups of documents will be conspicuously marked to ensure their protection to a degree as high as that of the most highly classified document therein. Documents separated from a file, folder, or group will be marked as prescribed herein for individual documents.

4-2. TRANSLATIONS:

Working papers and drafts will be marked with appropriate classification and declassification on instructions prior to submission for translation. They will be safeguarded IAW this regulation.

4-3. MISCELLANEOUS AND WASTE MATERIAL:

Classified material such as typewriter ribbons, carbons, waste and similar material, developed in connection with the handling processing, production, and utilization of classified information, will be protected in the same manner as other classified material. Computer disks and typewriter/printer ribbons used to process classified data will have affixed, in a prominent location, DA Label 89 (Top Secret), DA Label 90 (Secret), or DA Label 91 (Confidential), whichever is appropriate. In additional to the DA Label, a file imprinted with "ROKUS" will also be affixed. Destruction of such material will be effected as soon as possible. Unless a requirement exists to retain this type of material, there is no need to mark, stamp, or otherwise indicate that the recorded information is classified.

Chapter 5

ACCESS AND DISSEMINATION

5-1. ACCESS TO CLASSIFIED INFORMATION:

The dissemination of classified information verbally, in writing, or by any other means, will be limited to those persons whose official duties require knowledge or possession thereof. Access to classified information will not be authorized based on rank or position. The final responsibility for determining whether a person's official duties required that he possess or have access to any element or items of classified information, and whether he has been granted the appropriate security clearance by proper authority, rests upon each individual who has authorized possession, knowledge, or control of the information involved and not upon the prospective recipient.

a. Security Clearances: The UNC, ROK and U.S. Governments will provide their respective personnel with appropriate security clearances, based upon the requirements of the position occupied. The office of Industrial Security, Defense Investigative Service (OISI-FE, DIS) will certify the clearance status of U.S. contractor personnel authorized access to classified ROKUS material. The ACofS C2, will notify CFC, SM the clearance status of all assigned ROK military, ROK civilian employees of CFC, and all ROK contractor personnel requiring access to classified ROKUS material.

b. Access Roster: HQ, UNC/CFC and HQ, USFK/EUSA staff elements. SMs will maintain an up-to-date listing of personnel authorized access to classified material.

5-2. RESTRICTED AREAS:

Message centers, Tactical Operations Centers (TOC), crypto facilities, communications centers, and areas where TS-R information is stored will be declared "Restricted Areas". Security Managers will identify specific areas for designation as Restricted Areas and will submit request for designation to the USFK Provost Marshal, ATTN: PMJ-S. Bilingual restricted area signs will be posted on or near the restricted area entrance(s). Security Managers will ensure that access to designated "Restricted Areas" is strictly controlled.

5-3. CONTROLLED AREAS

Conference rooms (when classified information is being discussed) and other temporary-use areas will be designated as "Controlled Areas" by the appropriate user agency head. Access will be limited to personnel with an appropriate security clearance and need-to-know. Access rosters will be

provided by staff element SMs whenever a classified conference is planned. "Controlled Areas" signs (see appendix K) will be posted.

5-4. DISSEMINATION OF CLASSIFIED INFORMATION:

Heads of staff agencies will establish procedures for the dissemination of classified information originated or received by them, subject to specific rules established by this regulation. As a further limit on dissemination, the originating official or activity may prescribe additional specific restrictions on a classified document, or in its text, when security considerations make them necessary.

5-5. RELEASE OF ROKUS INFORMATION TO THIRD COUNTRIES:

No ROKUS information will be released to third countries without the prior approval of the Combined Forces Command, ACofS, C-2 and the USFK/EUSA ACofS, J2/G2. Proponent staff agencies will submit requests for approval of release to the HQ USFK/EUSA Foreign Disclosure Office (FKJ2-IS-S-F) and will maintain a record of release information to include a copy of the information released, date, and full justification therefore. Such records will be maintained by the proponent office for a minimum of 2 years.

5-6. RESTRAINT ON REPRODUCTION:

Classified material will be reproduced in minimum numbers and any originator stated prohibition against reproduction will be strictly observed. The following restrictive measures apply to reproduction equipment and to the reproduction of classified material:

a. The number of copies of documents containing classified information will be kept to a minimum to decrease the risk of compromise and reduce storage costs.

b. Heads of staff agencies and acting commanders or their designated representatives are authorized to approve the reproduction of classified information. These designated officials will carefully review the need for reproduction with a view toward minimizing classified reproduction consistent with operational requirements and reproduction prohibitions imposed by the originator or higher authority.

c. Security Managers will designate specific reproduction equipment for the reproduction of classified information. Reproduction of classified information will be restricted to equipment so designated. Rules to minimize human error, inherent in the reproduction of classified information, will be posted on or near the designated equipment (see appendix L).

d. An appropriate warning notice prohibiting reproduction of classified material will be posted by the security manager on equipment used only for the reproduction of unclassified material.

e. All copies of classified documents reproduced for any purpose are subject to the same controls prescribed for the original.

f. Written permission to reproduce TS-R documents must be obtained from the document originator.

g. Authorization to reproduce TS-R documents must be in writing. DA Form 3964 or other appropriate form may be used for this purpose.

5-7. CONTROL AND ACCOUNTABILITY:

The following administrative procedures are established to control all TS-R information and material originated or received by a combined staff agency; distributed or routed to components of, or activities within, the staff agency, regardless where located; or disposed of by the staff agency by transfer of custody or destruction.

a. Chiefs of each staff section creating, receiving, or handling classified ROKUS material will appoint, in writing, a Top Secret-ROKUS Control Officer (TSRCO) and alternate (if TS-R material is created, received, or handled). The Chief, Adjutant General Division, ACofS, C-1, is the TSRCO for HQ CFC.

b. Within combined activities, all classified TS-R information will be accounted for on DA Form 455 (appendix E). Control numbers will be assigned to each TS-R document consecutively beginning with the first document received each calendar year. Registers will be maintained for TS-R documents. Registers will list all pages containing TS-R information. Additionally, a stamp 1.5 cm high by 4.5 cm long will be stamped in the upper left hand corner in black on all TS-R documents, including changes (appendix D). Control numbers will be inserted within the space provided in the stamp. In addition, TSRCO's will initiate and maintain disclosure records (DA Form 969) on each TS-R document which contains the document title, or name and date of all individuals, including clerical personnel, who, during the period of custody, had access to the document. This does not include individuals within the staff agency who may simply have had access to containers in which TS-R information is stored. DA Form 969 will be retained within the staff section for 2 years after the documents are transferred, downgraded, or destroyed.

c. TS-R information and material will be under continuous receipt system at all times. Receipts shall be maintained for 5 years.

d. Destruction of classified documents and materials will be by burning, pulping, or shredding. The destruction of TS-R documents will be recorded on certificates of destruction. Certificates of destruction will be maintained for 2 years and will be numbered consecutively for each calendar year. Witnessing officials will sign only after having actually witnessed the destruction. The destruction official will ensure that complete destruction of classified waste has been accomplished.

e. An annual inventory of TS-R documents will consist of physical inspection by the TSRCO and a cleared disinterested witness of all TS-R documents present as of 1 April of each year, plus a verification by audit of all transactions involving TS-R documents which occurred during the preceding year or since the previous inventory. A separate inventory on 1 April of each year is not required if for any reason an inventory has been or will be conducted within 30 days before or after 1 April. The disinterested witness must not be in the chain of command of the TSRCO. Upon completion of the inventory/verification by audit, the TSRCO and disinterested witness will execute a certificate of inventor/verification by audit. The annual inventory/verification by audit certificate will be maintained by the TSRCO for two years (see appendix F).

f. A complete joint inventory of all controlled documents/material will be conducted upon change of TSRCO or in the event the TSRCO will be absent for any reason for a period in excess of 30 days, absent without leave, or hospitalized for a period of 30 or more days. In the latter event, the joint inventory will be conducted by the alternate TSRCO and a disinterested officer within 24 hours. The joint inventory will include physical sighting of the document, or verification of any transactions involving each controlled document. The joint inventory will be completed in time to allow resolution of any discrepancies before the departure of the outgoing TSRCO. A certificate will be executed by the incoming and outgoing TSRCO (see appendix G). The control numbers of the classified documents maintained by the staff agency will be listed on and become a part of the certificate of joint inventory.

g. During the first 10 days of June and December, the SM will ensure that at least 50 percent of all classified documents are reviewed for possible downgrading, declassification, destruction, and to ensure they contain proper classification markings. Each document maintained must be included in at least one biannual review per year. A certificate of each review will include number of accountable documents reviewed and an indication of action taken. The biannual review will be maintained in the staff agency's file for 2 years. This review is not to be confused with the required inventories. A review is conducted to determine the necessity for retaining the documents and to check for possible downgrading or declassification, whereas an inventory is designed to ensure that all documents are present or accounted for. One will not suffice for the other

h. Working papers are documents, including drafts, photographs, etc, accumulated or created to assist in the formulation and preparation of a finished document. Working papers containing classified information will be:

(1) Dated when created.

(2) Marked with the highest classification of any information contained in the document.

(3) Protected IAW the classification assigned.

(4) Destroyed when they have served their purpose.

(5) Accounted for, and controlled in the same manner prescribed for a finished document of comparable classification when:

(a) They contain TS information

(b) Placed permanently in a file system.

(c) Retained more than 90 days from the date of origin.

(d) Transferred outside of the office of origin.

5-8. DISPOSAL AND DESTRUCTION:

All classified material will be destroyed by a properly cleared individual, in the presence of an appropriate witnessing official when required, by burning, pulping, or shredding. Shredded material size must not exceed 1/32" x ½" crosscut. Records of destruction are required for TS-R material, and will be dated and signed by the destruction official and a disinterested witness. Witnesses will not be in the chain of command of the TS-R custodian. Certificates of destruction will be sequentially numbered by year, and classification category; i.e., CD-TSR-1-97, CD-TSR-2-07, etc.

Chapter 6

SAFEKEEPING AND STORAGE

6-1. GENERAL:

Classified information/material may be used, held, or stored only where there are facilities or conditions adequate to prevent unauthorized persons from gaining access.

6-2. STORAGE OF CLASSIFIED MATERIAL:

Whenever classified ROKUS material is not under the personal control and observation of an authorized person, it will be guarded by appropriately cleared personnel or stored in a locked security container, vault, or secure room approved for that purpose by the ACofS, C-2.

a. Safekeeping and Storage of TS-R: TS-R material will be stored in facilities approved by the ACofS, C-2, meeting the following minimum requirements.

(1) In a safe or security container approved by the U.S. General Services Administration, having a built-in, three position, dial-type combination lock meeting Federal Specifications.

(2) Supplemental area controls consisting of a substantially constructed and secured building or room, locked and either guarded or alarmed. Windows, if any, must be barred and any ducts, trap doors, or similar miscellaneous openings must be secured from the inside. Doors will be solid wood or metal plated and secured by a three-position dial-type changeable combination pad lock and heavy duty hardware. Guards, if any, must be either U.S. or ROK citizens, but if positioned external to the building, vault, or room, need not have a security clearance. The guard may be a building guard, such as a "CQ" or duty officer. He need not be armed, and continual surveillance of the room is not required.

(3) All persons authorized unescorted access to TS-R containers, even when locked, must have TS clearances.

b. Secret-ROKUS: S-R information and material will be stored in any container of facility approved for TS-R or a vault, vault type room, or strong room, which has been approved for open storage by the ACofS, C2. In addition, it may be stored in any steel filing cabinet having a built, three position, dial combination lock.

c. Confidential-ROKUS: C-R may be safeguarded in any storage container or area authorized for S-R. In addition, C-R may be safeguarded in any storage cabinet, supply cabinet or filing cabinet that can be locked, and which is further secured in a locked or guarded building or room.

d. When classified storage containers are stored in any van, vehicle, or other mobile unit, provisions will be made to preclude theft of the entire mobile unit.

6-3. MASTER CLASSIFIED STORAGE CONTAINER:

Each security manager will designate a master classified storage container for his activity. Only the security manager and his designated representatives will know the combination to the master classified storage container. The master classified storage container will be utilized to store the combinations of all storage containers within the organizational element. The combination to the Master Storage Container will be stored in another elements approved master storage container within the same building if possible.

6-4. CLASSIFIED STORAGE EXCEPTION:

a. Funds, valuables, narcotics, weapons/ammunition, sensitive items or the keys/combinations to containers containing such items will not be stored in any container utilized to store classified information and material.

b. The storage of classified components of weapon systems, keys/combinations which allow or disclose a means of access to classified weapons/ammunition, and classified communication equipment will be stored in classified containers.

6-5. CONTAINER IDENTIFICATION AND COMBINATIONS:

a. Identification: Each storage container used for the storage of classified information or material will be assigned a number for identification purposes. The number will be affixed in a conspicuous location on the front of the container. Manufacturer attached metallic number plates found on most modern security containers meet this requirement. The contractor number will also be recorded on SF Form 700 which will be affixed to the inside of the combination drawer of each classified container and on SF Form 702 affixed to each container.

b. Combinations: Combinations to security containers will be changed only by individuals having the appropriate security clearance. Combinations will be changed under any of the following circumstances:

(1) When a container is placed in use.

(2) Whenever an individual knowing the combination no longer requires access.

(3) When the combination of record of combination has been compromised or the security container has been discovered unlocked and unattended.

(4) At least annually unless more frequent change is directed by the type material stored therein.

(5) When taken out of service. Built-in combination locks will be reset to the standard combination 50-25-50; combination padlocks will be reset to the standard combination 10-20-30

c. Classifying Combinations: The combination of a classified storage container used for storage of classified material will be assigned a security classification equal to the highest category of the classified material authorized to be stored therein.

d. Classified storage container record: A record will be maintained for each classified storage container, including vaults and strong rooms, showing location of container, and the names , home addresses, and home telephone numbers of at least two, but not more than four persons having knowledge of the combination (see appendix M).

e. Dissemination: Knowledge of or access to the combination of a classified storage container will be given only to those appropriately cleared persons who are authorized access to all the information stored therein.

f. Changing Combinations and Repairs: Uncleared personnel will not be permitted to change the combinations of security containers utilized for the storage of classified information or material. Only U.S. or ROK government agencies or personnel, and contractors approved by the U.S. or ROK government may repair government security containers.

6-6. CARE DURING WORKING HOURS:

a. Each individual will take precautions to prevent access to classified information by unauthorized persons. Classified documents, when removed from storage for working purposes, will be kept under constant surveillance, and covered with a classified document cover sheet when not in use.

b. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, typewriter ribbons and all similar document production items containing classified information will be destroyed as soon as possible when no longer needed or given the same

classification and safeguarded in the same manner as the classified material produced from them.

6-7. CARE AFTER WORKING HOURS:

a. Head of agencies will required a system of security checks at the close of each working day to ensure that the classified material held by the activity is properly protected. They will require the security managers or designated official to make, or cause to be made, an inspection to ensure, as a minimum, that:

(1) All classified material is stored in the prescribed manner.

(2) Classified waste is properly stored or destroyed.

(3) Classified shorthand notes, carbon paper and plastic typewriter ribbons, drafts, and similar papers have been properly stored or destroyed. As a matter of routine during the day, such items will be placed in a classified waste container immediately after they have served their purpose.

b. Personnel locking or unlocking security containers must be cleared for the highest degree of classified material stored therein. Anyone may double check the container except the person who locked it. No clearance is required, but when an uncleared person double checks the container, the person who locked the container must be present. Containers will be checked, and SF Form 702 (Security Container Check Sheet), initialed, at the close of each working day even if the container was not opened. In such a case the "unlocked by/locked by" column will be lined through. Containers will be checked as soon as possible after the container is locked. As an exception Individuals working alone or after normal duty hours will be authorized to initial the double check themselves.

6-8. EMERGENCY PLANNING:

a. Emergency plans for protection, removal, and/or destruction of classified material will be prepared by each activity SM, under separate cover.

b. The ACofS, C-2 will provide basic guidance to all activities. In turn, each activity SM will use the guidance to delineate the particular requirements for each office. A copy of each activities emergency plan will be provided to the ACofS, C-2.

c. Emergency plans will be updated annually or as changes occur.

d. Emergency plans will be conspicuously posted on each security container.

6-9. SECURITY OF MEETING AND CONFERENCES:

When arranging classified conferences or meetings, consider necessary security measures, Ensure:

a. Each person attending has the appropriate security clearance and need-to-know.

b. Identity of attendees and their level of access is provided beforehand by their SM, and checked against a roster at the conference.

c. That the area in which classified information is to be discussed affords adequate security against unauthorized physical, audio, or visual access.

d. Adequate storage facilities are available.

e. Classified material furnished to those in attendance is under control and safeguarded.

f. The classification of the discussion is announced at the beginning and end of the conference and at appropriate intervals during the conference.

g. That discussions are limited to the level authorized. Post signs announcing the classification of the conference are posted in conspicuous locations inside the conference room.

h. That that area is properly secured and guarded during breaks.

i. That the area is checked carefully for notes and other classified materials possibly left behind at the end of the conference.

Chapter 7

COMPROMISE OF CLASSIFIED INFORMATION

7-1. GENERAL:

The compromise of classified information presents a threat to mutual security. The seriousness of that threat must be determined and appropriate measures taken to prevent, negate or minimize the adverse effect of such a compromise. Simultaneously, action must be taken to regain custody of the material if lost, and to identify and correct the cause of the compromise.

7-2. RESPONSIBILITY OF DISCOVERER:

Any person who has knowledge of a security violation, the actual or possible compromise of classified information will immediately report the circumstances to his SM.

7-3. PRELIMINARY INQUIRY:

The SM of the staff section or agency where the incident occurred will appoint a preliminary inquiry officer to conduct a preliminary inquiry to determine the circumstances and the probability of compromise and fix initial responsibility. If another agency or activity was responsible for the violation, responsibility for completing the preliminary inquiry will be passed to that activity as soon as possible. a written report will be provided to the gaining SM and a copy will be forwarded to ACofS, C-2, ATTN: CFCB-IS-S-IPS. Whenever possible, security violations or possible compromises will be resolved in the course of the preliminary inquiry. The report, in the form of a memorandum, will be addressed to the chief of the responsible staff section or agency, who will take appropriate corrective action, including punitive action, if necessary. A copy of the report, together with a statement of corrective and/or action taken or recommended will be furnished the ACofS, C-2, ATTN: CFCB-IS-S-IPS. The ACofS, C-2 will review the report for adequacy and completeness and may recommend further investigation or additional corrective actions.

7-4. INVESTIGATION.

If the preliminary inquiry officer cannot determine the probability of compromise, the cause of the incident, or fix responsibility as a result of the Preliminary Inquiry, a formal investigation will be initiated. The responsible staff principal, or agency will request the commander, 34TH SUPPORT GROUP, ATTN: EANC-SA-O to appoint a disinterested investigating officer, superior in rank to all persons possibly responsible for the incident, to conduct the investigation under the formal procedures of AR 15-6. If ROK personnel were involved in the incident, an additional ROK

Officer of equivalent or higher rank will be appointed by ACofS, C-2. The investigating officers will ensure compliance with ROK investigative principals as well as U.S.

7-5. RESPONSIBILITY OF AUTHORITY ORDERING INVESTIGATION:

The report of investigation will be reviewed by the head of the responsible agency. The findings and recommendations will be reviewed and appropriate remedial, administrative or disciplinary action will be taken. A copy of the report of investigation and action taken will be forwarded to the ACofS, C-2.

7-6. ESPIONAGE AND DELIBERATE COMPROMISE:

U.S. personnel who become aware of incidents of possible espionage or deliberate compromise of classified information will contact the nearest field office of the 524TH MI BN or CFCB-IS-C as soon as possible. ROK personnel will report to appropriate ROK agencies.

Chapter 8

TRANSMISSION AND TRANSPORTATION

8-1. TOP SECRET-ROKUS

TS-R will be physically transmitted only by:

a. Hand carry by the officials involved (the drafter, signer, custodian, etc.)

b. Appropriately cleared, designated courier.

c. U.S. Armed Forces Courier Service or ROK equivalent.

d. TS-R information/material may not be sent through the postal system.

e. TS-R will be kept under a continuous receipt system. Receipts must be executed when the information/material changes custodian accounts, goes from one office to another, or from one individual to another.

f. Except when being hand carried by the officials involved between buildings on the same installation, TS-R documents will always be double wrapped and sealed and will be transported in a locked briefcase-type container.

g. Only a TSRCO, alternate TSRCO, or the staff section SM may receipt for TS-R documents.

8-2. SECRET-ROKUS AND CONFIDENTIAL-ROKUS.

S-R and C-R material may be physically transmitted in the same manner prescribed for TS-R documents. Couriers will be designated in writing by the SM. Couriers will be either American or Korean citizens, of any rank or grade, with an appropriate clearance. Travel orders if issued will include authorization to carry classified material. If the designated courier is other than the originator, or his representative, the courier will receipt for the document. If the document is in a sealed envelope or pouch, the courier need only sign for the sealed envelope or pouch. If the document is not in a sealed envelope it will be covered with an appropriate cover sheet and will be transported in a pouch, briefcase, portfolio, opaque envelope or folder. If it is being carried in a sealed envelope with appropriate classification markings, the envelope will be placed in an outer opaque envelope which will not be marked with classification markings. No escort is required for the designated courier. Under no circumstances will classified material being transmitted be allowed out of the sight of the designated courier unless a receipt for the material is obtained, such as when the material will be

held in temporary storage overnight. S-R and C-R may be transmitted by registered mail and through routine message center channels (classified distribution). When delivered to a message center for distribution, the outer envelope will be sealed only by the Message Center personnel.

8-3. MOVEMENT OF SECRET-ROKUS AND CONFIDENTIAL ROKUS MATERIAL:

When classified material is being transmitted in a military vehicle, the designated courier will carry the material with him in the cab, if possible. If the material is of such size or volume that it must be transmitted in the back of a vehicle such as a truck or van, it will be locked in a security container which is chained and padlocked to the body of the vehicle if possible. If the material is bulky and does not permit locking in a security container, then it shall be crated and security banded. During the movement, the vehicle will be followed by another military vehicle for the express purpose of preventing unauthorized entry from the rear. Classified material being transported in a military sedan may be locked in the trunk while the vehicle is in transit, but at not time will the vehicle be left unattended while the material is stored therein.

8-4. ADDRESSING

Addresses on both the inner and outer envelopes will be full and complete and will include an attention line. Unfamiliar abbreviations will not be used.

8-5. PREPARATION OF MATERIAL FOR TRANSMISSION OR SHIPMENT.

Whenever classified information is transmitted, it will be enclosed in two opaque sealed envelopes or similar wrappings where size permits, except as provided below:

a. Whenever classified material is too large or bulky to be transmitted as above, it will be enclosed in two opaque sealed containers, such as boxes or heavy wrapping. So long as this requirement is observed, the materials my be wrapped, boxed, or crated or a combination thereof. Boxed or packaged material will be sealed with package sealing tape and banded, if possible.

(1) If the classified material is an internal component of a packageable item of equipment, the outside shell or body may be considered as the inner enclosure.

(2) If the classified material is an inaccessible internal component of a bulky item or equipment that can not be reasonably packaged, the outside or body of the item may be considered as the other enclosure provided the shell or body is not classified.

(3) If the classified material is an item of equipment that is not reasonably packageable and the shell or body is classified it will be draped with an opaque covering that will conceal all classified features. Such coverings must be capable of being secured so as to present inadvertent exposure of the item.

(4) Specialized shipping containers, including closed cargo transporters, may be used in lieu of the above. In such cases, the container may be considered the outer wrapping or cover.

b. Material used for packaging will be of such strength and durability as to provide security protection while in transit to prevent items from breaking out of the container and to facilitate the detection of any tampering with the container. The wrapping will conceal all classified features.

c. Closed and locked compartments, vehicles or cars will be use for shipments of classified material except when another method is authorized by the ACofS, C-2.

d. To minimize the possibility of compromise of classified material caused by improper or inadequate packaging thereof, SMs will ensure that proper wrappings are used for mailable bulky packages. Staff agencies will stock several sizes of cardboard containers and corrugated paper. SMs will require the inspection of bulky packages to determine whether the material is suitable for mailing or whether it should be transmitted by other approved means.

8-6. WRITTEN MATERIAL

Classified written material will be folded or packaged in such a manner that the text will not be in direct contact with the envelope or container. A receipt form will be attached to or enclosed in the inner envelope or container for all classified material. The mailing of written material of different classification levels in a single package will be avoided when possible. However, when written materials of different classifications are transmitted in one package, they will be wrapped in a single inner envelope or container. A receipt listing all secret or higher material will be attached or enclosed. The inner envelope or container will be marked with the highest classification of the contents. The inner envelope or container will show the address of the receiving activity and classification, including (where appropriate) special markings or instructions. It will be carefully sealed to minimize the possibility of access without leaving evidence of tampering. An outer container will show the complete and correct address and the and the

return address of the sender. The outer cover of container will not bear a classification marking, a listing of the contents divulging classified information, or any unusual data or marks which might invite special attention to the fact that the contents are classified. It will NOT be marked with an individual's name.

8-7. EXCEPTION

Exceptions to methods of transmission or transportation may be authorized by the ACofS, C-2, provided the exception affords equal or greater protection and accountability to that provided above. Exceptions to policy will be submitted to the ACofS, C-2, ATTN: CFCB-IS-S-IPS in a timely manner to allow full evaluation of the alternative(s) proposed.

Chapter 9

DOWNGRADING, DECLASSIFICATION, AND DESTRUCTION

9-1. GENERAL

When classifying a document, it is necessary to determine how long the classification should last. The policy is set forth in Appendix B. Classified information and material shall be downgraded, declassified, or destroyed as soon as there are no grounds for continued classification/retention.

9-2. DISPOSAL AND DESTRUCTION

All classified material will be destroyed by burning, pulping, or shredding. Records of destruction are required for TS-R material, and will be dated and signed by the destruction official and at least one properly cleared witness. Certificates of destruction will be sequentially numbered beginning with "1" at the start of each calendar year i.e., CD-1-97. See Appendix I for sample. Any properly cleared person may destroy or witness destruction of classified material. Appointment orders are not required. Material containing S-R and C-R information is not accountable; and may be destroyed without regard to accountability.

Chapter 10

SECURITY EDUCATION

10-1. GENERAL

Heads of staff elements and activity commanders are responsible for establishing security education programs for their personnel. The security education program will include all personnel entrusted with classified information regardless of their position, rank, or grade. Each activity will design its programs to fit the particular requirements of the different groups of personnel who have access to classified information. The program will be designed to:

a. Advise personnel of the need for protecting classified information and the adverse effects to mutual security resulting from compromise.

b. Indoctrinate personnel fully in the principles, criteria, and procedures for the classification, declassification, safeguarding, destruction or transfer of material.

c. Familiarize personnel with the specific security requirements of their particular assignment, and require them to execute a briefing statement prior to granting access. A sample briefing statement is at Appendix N.

d. Inform personnel of the techniques employed by enemy intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

e. Advise personnel of the hazards involved and the strict prohibition against discussing classified information and their responsibility for reporting such attempts.

f. Advise personnel of the disciplinary actions that may result from violation of this regulation.

10-2. REFRESHER BRIEFING:

Positive programs will be established to provide annual security training for personnel having continued access to classified information. The elements outlined in paragraph 10-1, above, will be updated and tailored to fit the needs of experienced personnel.

10-3. BRIEFINGS

The SM or his designated representative will conduct all security briefings.

10-4. INSPECTION CHECKLIST:

A security checklist in included as Appendix O for guidance.

Chapter 11

제 11 장

REFERENCES

참고문헌

11-1. REFERENCES:

a. Ministry of National Defense (MND) order #351, (Military Security Function Regulation).

가. 국방부 훈령 351 호(군사 보안업무시행규칙)

b. DoD Regulation 5200.1-R Information Security Program Regulation

나. 미 국방성 보안규정 5200, I-R 정보보안 규정

C. Army Regulation 380-5 Information Security Program Regulation

다. 육군 규정 380-5 정보보안 규정

d. Executive Order 12958, Classified National Security Information.

라. 미 대통령령 12958, 국가 비밀 정보보안 규정

The proponent for this regulation is the Assistant Chief of Staff, C-2. Users are invited to send comments and suggested improvements on DA Form,2028 (Recommended Changes to Publications and Blank Forms) or other appropriate correspondence to ACofS, C-2, ATTN: CFCB-IS-S-IPS, APO, AP 96205.

본 규정의 발의부서는 연합사 정보참모부이다. 사용부서에서 의견 및 개선사항이 있을 시에는 미 육군양식 2028(간행물 및 양식에 개정 건의사항 명시)또는 기타 적절한 문서로 연합사 정보참모부 보안과에 제출한다(APO AP96105)

FOR THE COMMANDER IN CHIEF:

사령관을 대리하여

OFFICIAL:

HWANG, Il Myun
COL,ROKA
Adjutant General, CFC

황 일 면
대한민국 육군 대령
연합사 부관처장

DANIEL J. PETROSKY
LTG, USA
Chief of Staff, UNC
Chief of Staff, CFC

제임스 에프. 페트로스키
미 육군 중장
유엔사/연합사 참모장

DISTRIBUTION:

"A"

APPENDIX A

SAMPLE APPOINTMENT FORMAT

ROK-U.S. COMBINED FORCES COMMAND

"Office Symbol"
"Date"

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Additional Duty Appointment, Security Manager (Name of Appointee)

1. You are hereby appointed as (type of appointment) for (Staff Agency), effective (date), IAW UNC/CFC Reg 380-1, para 1-3. This appointment supercedes all previous appointments and expires on (date).

2. You must familiarize yourself with the provisions of UNC/CFC Reg 380-1 and all other applicable regulations.

"SIGNATURE BLOCK"
"Head of Staff Element"

DISTRIBUTION
1 - Individual Concerned
1 - Unit of Assignment
1 - Custodian of Personnel records
1 - CFCB-IS-S-IPS

APPENDIX B

CLASSIFICATION CRITERIA, POLICIES, CONSIDERATIONS

1. GENERAL:

The determination of classification requires balanced judgment. Both advances and disadvantages must be considered prior to making a classification decision.

a. Classification Determination: Classification determination must be preceded by an exact identification of each item of information that may require security protection in the interest of national security. This process involves identification of that specific information which provides advantage to ROKUS and would or could result in damage to mutual security in the event of unauthorized disclosure.

b. Evaluation of information: A document or other material is classified based on evaluation of the material and either:

(1) Because direct study, analysis, observation, or use of the material would reveal information where the unauthorized disclosure thereof could result in damage to national security.

(2) Because information may reveal when associated with other information, to include information already released into the public domain.

c. Specific classifying criteria: A determination to classify will be made only when one or more of the following considerations are present and the unauthorized disclosure of the information could reasonable be expected to cause a degree of harm to the mutual security of the US and ROK.

(1) The information provides the US and the ROK with a strategic or tactical advantage directly related to mutual security.

(2) Disclosure of the information would weaken the position of the UA and the ROK in the course of international discussions or negotiations, generate a military threat to the US or the ROK, create or increase international tensions, result in s disruption in foreign relations, or lead to hostile political or military action against the US or the ROK.

(3) Disclosure of the information would weaken the ability of the US or the ROK to wage war or defend either nation successfully or make either nation vulnerable to attack.

(4) There is a sound reason to believe that other nations do not know that the US or ROK have or are capable of obtaining certain information or material which is important to the mutual security.

(5) There is a sound reason to believe that the information would:

(a) Provide a foreign nation with insight into the war potential or the effectiveness of defense plans or posture of the US and ROK.

(b) Allow a foreign nation to develop, improve, or refine a similar item of war potential.

(c) Provide a foreign nation with a base upon which to develop effective countermeasures.

(d) Weaken or nullify the effectiveness of a defense or military plan, operation, project, or activity vital to the mutual security.

2. CLASSIFYING DOCUMENTS:

Each document will be classified on the basis of the information it reveals. The fact that a document makes reference to a classified document is not the basis for classification unless the reference, standing alone, reveals classified information. The overall classification of a document, file, or group of connected documents will be a least as high as that of the highest classified component. Each component, however, will be classified individually on its own merits. The subject or title of a classified document should normally be unclassified for ready reference. When the information revealed by a subject or title warrants classification protection, an unclassified short title will be added for reference purposes.

3. CLASSIFYING MATERIAL OTHER THAN DOCUMENTS:

Items of equipment or other physical objects may be classified only when classified information may be derived from them by visual observation of internal or external appearance, structure, operation, test, application, or use. The overall classification assigned to equipment or physical objects will be at least as high as the highest classification of any of the items of information revealed by the equipment or objects.

4. AFFECT OF OPEN PUBLICATIONS:

Appearance in the public domain of information currently assigned or being considered for classification does no preclude initial or continued classification; however, such disclosures require immediate re-evaluation of the information to determine if downgrading or declassification is warranted.

5. RE-EVALUATION OF CLASSIFICATION BECAUSE OF COMPROMISE:

Specific classified information subjected to compromise or possible compromise and information related thereto will be re-evaluated and acted upon as follows:

The original classifying authority, upon learning that a compromise or probable compromise of specific information has occurred, will:

a. Re-evaluate the information involved and determine whether:

(1) The classification should be continued without changing the specific information involved.

(2) The specific information or parts thereof, should be modified to minimize or nullify the effects of the reported compromise and the classification retained.

(3) Immediate downgrading or declassification is appropriate.

(4) The original date specified for declassification of the information involved should be changed to reflect an earlier declassification date.

(5) One of the above courses of action should be taken or, in lieu thereof, upgrading of the related information is warranted.

b. When such determination is within subparagraphs 5a(2) through (5) above, prompt notice is required to all holders of such information.

c. When classified information has been compromised, but the compromise cannot reasonably result in damage to mutual security, the above evaluation is not required.

6. EXTRACTS OF INFORMATION:

Information or material extracted from a classified source will be classified, or not classified IAW the classification markings shown in the source document. The overall marking and internal marking of the source should supply adequate classification evidence to the person making the extraction. However, if internal markings are lacking, no classification guidance is included in the source, no reference is made to applicable classification guidance is included in the source, and no reference is made to an applicable classification, the extracted information or material will be classified to correspond to overall marking of the source, or IAW guidance specifically sought and received from the classifier of the source material.

7. CLASSIFICATION GUIDES:

A classification guide, based upon classification determination made by appropriate classification authorities, will be issued for each system, program, project or operation. Successive operating echelons may prescribe any further detailed supplemental guidance deemed essential to ensure accurate, uniform and consistent classification.

APPENDIX C

ORIGINAL CLASSIFICATION AUTHORITY

TOP SECRET-ROKUS:
CINC, United Nations Command (UNC)/ROK-US Combined Forces Command (CFC).
SECRET-ROKUS/CONFIDENTIAL-ROKUS:

a. CINC, UNC/CFC.

b. Deputy Commander in Chief, CFC.

c. Deputy Commander in Chief, UNC.

d. Chief of Staff, CFC.

e. Deputy Chief of Staff, CFC.

f. Commander, Naval Component Command.

g. Commander, Air Force Component Command.

h. Senior Member, UNC Military Armistice Commission.

i. Special Advisor to Commander in Chief, UNC.

k. Commander, UNC Rear.

l. ACofS, C1, CFC.

m. ACofS, C2, CFC.

n. ACofS, C3, CFC.

o. ACofS, C4, CFC.

p. ACofS, C5, CFC.

q. ACofS, C6, CFC.

r. ACofS, Engineer, CFC.

APPENDIX D

SAMPLE CLASSIFICATION/CONTROL NUMBER STAMPS, AND CONTROL NUMBERS

1. CLASSIFICATION STAMPS:

(KOREAN)
TOP SECRET-ROKUS

7 cm 1.5 cm RUBBER STAMP

(KOREAN)
SECRET-ROKUS

7 cm 1.5 cm

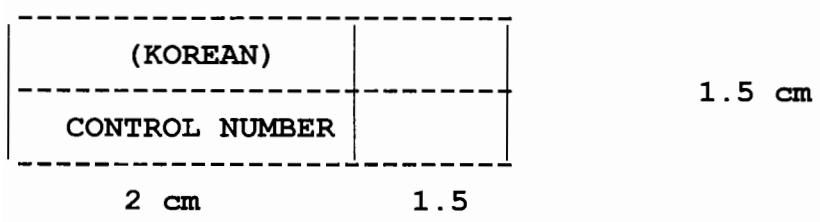
(KOREAN)
CONFIDENTIAL-ROKUS

7 cm 1.5 cm

(KOREAN)
UNCLASSIFIED-ROKUS

7 cm 1.5 cm

2. CONTROL NUMBER STAMP



3. CONTROL NUMBER EXAMPLES:

a. The first TOP SECRET-ROKUS received in a calendar year will show the following control information:

STAFF AGENCY	CLASSIFICATION	YEAR	DOCUMENT NUMBER.

The following would be an example of what the ACofS, C2's control information would look like for the first TOP SECRET-ROKUS document received in 1998:

ACofS, C2	TS-R	1998	001

CONTROL, LOG OR FILE NO.	DATE REC'D	CLAS S	NO. OF CYS	DESCRIPTION (Type, File Reference, Unclassified Subject or Short Title, No. of Pages, Copy Numbers, etc.)	ORIGINATING AGENCY	DATE OF DOCU-MENT	ROUTED TO	REMARKS (Disposition, Dest'n Cert No. and Date, Custodian Signature, etc.)

DA FORM 1 JUL 62 455 REPLACES EDITION OF 1 JAN 57, WHICH IS OBSOLETE.

PPC-Korea

MAIL AND DOCUMENT REGISTER PAGE NO.

For use of this form, see AR 380-5; the proponent agency is Office of the Assistant Chief of Staff for Intelligence.

APPENDIX F

SAMPLE CERTIFICATE OF ANNUAL INVESTORY/VERIFICATION BY AUDIT (TS-R)

ROK-US COMBINED FORCES COMMAND

(Office Symbol) Date

Certificate of Annual Inventory/verification by Audit
(TOP SECRET-ROKUS)

We, the undersigned, have conducted the annual inventory/verification by audit of all TS-S documents maintained by this account. All TS-R documents were present or properly accounted for.

Signature Block
(Disinterested Witness)

Signature Block
(TS-R Control Officer)

APPENDIX G

CLASSIFIED DOCUMENT ACCOUNTABILITY RECORD

1. A DA Form 3964 (Classified Document Accountability Record) will be used to control TOP SECRET-ROKUS documents. This multipurpose classified document accountability record can be used for a single or multiple document receipting, suspense control, internal routing, reproduction authorization, tracer actions for documents transferred, and a certificate of destruction when documents have served their intended purpose. The following are the most common uses of the form, and the appropriate sections to be completed for each use:

a. To use for internal receipting, complete sections A and B.

b. To use for external receipting, complete section A. Recipient completes section B.

c. To use for suspense control, fill out the appropriate blocks in section A.

d. To use for document destruction, complete sections C, and section A. if not already completed.

e. To use for reproduction authorization, complete section D.

f. To use for tracer action, complete section E. and section A. if not already completed.

APPENDIX H

SAMPLE CERTIFICATION OF BIANNUAL REVIEW

ROK-US COMBINED FORCES COMMAND

Office Symbol Date

Certificate of Biannual Review

I certify that I have completed a biannual review of 50 percent of all classified holdings and that all documents retained are for necessary operations. Documents found unnecessary have been destroyed or transferred.

Control Number	Disposition
	Present
	Destroyed

Signature Block
Security Manager

Appendix I. Daily Security Checklist

MONTH/YEAR		DAILY SECURITY CHECKLIST	STATEMENT :I have conducted a security inspection of this work area and checked all the items listed bellow
BLDG.NO	RM.NO		

I T E M	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Desk. wastebaskets and other surfaces and receptacles are free of classified meterial																															
2. Security containers have been locked and checked																															
3. Window and doors have been locked																															
4. Typewriter ribbons and ADP devices(e.g,diskettes,tapes) containing classified mater -al have been romoved and properly secured																															
5. security alarm(s) and equipment have been activated (where appropriate)																															
INTIALS OF CHECKER																															
TIME CHECKED																															

NOTE : Irregularities discovered will be promtly reported to the designated Security office for corrctive action

CHQ FORM 113 1 AUG 91

APPENDIX J

SAMPLE RESTRICTED AREA SIGN

TEXT IN KOREAN	WARNING (RESTRICTED AREA) ACCESS TO THIS AREA IS LIMITED TO AUTHORIZED PERSONNEL WHO HAVE AN APPROPRIATE SECURITY CLEARANCE AND NEED-TO-KNOW. ALL UNAUTHORIZED PERSONNEL WHO REQUIRE ACCESS WILL BE ESCORTED BY SPONSORING OFFICIAL.

APPENDIX K

SAMPLE CONTROLLED AREA SIGN

TEXT IN KOREAN	WARNING (CONTROLLED AREA) ACCESS TO THIS AREA IS LIMITED TO PERSONNEL WHO HAVE A_____ SECURITY CLEARANCE AND NEED-TO-KNOW

APPENDIX L

SAMPLE REPRODUCTION MACHINE AUTHORIZATION SIGH

This reproduction machine is authorized for the reproduction of classified documents up and including (CLASSIFICATION LEVEL). Operators will ensure that: (1) no one without a security clearance and need-to-know can view the reproduction of classified documents; (2) all pages are turned face down when not in use; (3) a minimum number of copies are made; (4) a thorough search of the area is conducted upon completion of reproduction to ensure that all classified information is removed; (5) any waste generated is properly safeguarded and/or destroyed.

APPENDIX M

CLASSIFIED STORAGE CONTAINERS

1. CLASSIFIED STORAGE CONTAINER RECORD. SF Form 700 (Classified Container Information) will be used to record the combination of classified containers and the names and addresses of persons knowing the combinations.

a. Part "1" will contain the names, addresses, and telephone numbers of at least two, but no more than four people with access to that container, location and identification of the container, and the date the combination was changed. It will be attached to the inside of the combination drawer of the container.

b. Part "2", which serves as an envelope for the combination, will contain the same information as Part "1". Part "2A" will contain the combination will be secured in the Part "2" envelope. Both Part "2" and "2A" must be stamped with the highest level of classification contained in the container, and maintained within the staff section master classified storage container

2. COMBINATIONS. The classified storage container record will be completed immediately after the change of the combination, and disposition made accordingly.

APPENDIX N

SAMPLE SECURITY BRIEFING STATEMENT

ROK-US COMBINED FORCES COMMAND

Office Symbol Date

Security Briefing Statement

I have been fully briefed and have read UNC/CFC Reg 380-1 and is familiar with the requirements set forth in this regulation as they pertain to my job.

Signature Block
of Individual Briefed

NOTE: This statement will be maintained by the security manager responsible for the briefing.

APPENDIX O

UNC/CFC SECURITY INSPECTION CHECKLIST

	YES	NO	NA
1. Does each Security Manager have a copy of UNC/CFC Reg 380-1?	___	___	___
2. Is the security manager and alternate appointed in writing IAW Appendix A, and do they meet the Grade requirements? (para 1-3c)	___	___	___
3. Has the security manager established procedures to ensure that all personnel who handle classified material are properly trained? (para 1-3c(1),(c))	___	___	___
4. Has the security manager executed a program of document review to eliminate unneeded classified material? (para 1-3(1),(e)	___	___	___
5. Has security manager conducted security inspections and spot checks, and are records maintained accordingly? (para 1-3c(1),(i)	___	___	___
6. Is the security manager senior in rank to the TS-R Control Officer? (para 1-3c(1),(h)	___	___	___

	YES	NO	NA
7. Are classified documents, including parts thereof, properly marked with assigned classification? (para 3-1)	___	___	___
8. Has a TS-R Control Officer been appointed in writing and does he/she meet the minimum grade requirements? (para4-1a)	___	___	___
9. Do containers used to store classified material meet minimum standards (para 6-2)	___	___	___
10. Is TOP SECRET-ROKUS material stored in buildings/rooms that meet minimum standards? (para 6-2a(2)(3))	___	___	___
11. Is a master classified storage container identified/used? (para 6-3)	___	___	___
12. Are classified containers marked for identification purposes? (para 6-5)			
13. Are combinations changed IAW para 6-5b(1) thru (5)?	___	___	___
14. Is the classified storage container record properly completed and posted? (para 6-5b and appendix M)	___	___	___
15. Has end-of-day security checks been established and implemented? (para 6-7a)	___	___	___

	YES	NO	NA
16. Is the security container check-list (SF702) properly maintained? (6-7b)	___	___	___
17. Has an emergency evacuation and destruction plan been written?	___	___	___
a. Is it posted on each classified container?	___	___	___
b. Does it meet minimum requirements?	___	___	___
c. Is it updated annually? (para 6-8a,b,c and d)	___	___	___
18. Are access rosters maintained for personnel authorized access to classified information? (para 5-1c)	___	___	___
19 Has reproduction equipment used to reproduce classified information been designated by the security manager and are the rules for use posted near the equipment? (para 5-6)	___	___	___
20. Is an accountability system for TS-S documents implemented and maintained?	___	___	___
a. Are control numbers assigned?	___	___	___

	YES	NO	NA
b. Are all classified pages listed on registers?	___	___	___
c. Are assigned control numbers listed on all documents?	___	___	___
d. Are disclosure records maintained for each TS-R document?	___	___	___
e. Are disclosure records maintained for two years? (para 4-1a thru f)	___	___	___
21. Are TS-S documents under a continuous receipt system? (para 4-1c)	___	___	___
22. Are certificates of destruction maintained for all TS-R documents destroyed? (para 4-1d)	___	___	___
23. Has an annual inventory and verification by audit been conducted on all TS-S on hand?	___	___	___
a. Has accountability been accomplished as of 1 April each year?	___	___	___
b. Has the audit included all transactions which occurred during the previous year? (para 4-1d)	___	___	___

	YES	NO	NA
24. Was the annual inventory/ verification witnessed by a disinterested officer? (para 4-1d)	___	___	___
25 Are inventories/verification by audit maintained by the TS-R Control Officer for two years? (para 4-1d)	___	___	___
26. Are joint inventories conducted upon change of custodian and/or when otherwise required? (para 4-1e)	___	___	___
27. Are bi-annual reviews conducted of at least 50 percent of all classified material within the first ten days of June and December? (para 4-1g)	___	___	___
28. Are working papers formulated, handled, transferred and destroyed as required? (para 4-1h(1))	___	___	___
29. Are CFC classified couriers appointed on orders? (para 8-2)	___	___	___
30. Are TS-S material transmitted as required? (para 8-1)	___	___	___
31. Is a security program established and does it meet minimum requirements? (para 10-1)	___	___	___

APPENDIX P

SAMPLE PRELIMINARY INQUIRY

CFCB-IS-S-IPS

"Date"

MEMORANDUM FOR Assistant Chief of Staff, C2, ATTN: CFCB-IS-S
APO, AP 96205

SUBJECT: Preliminary Inquiry

1. At 0815 hours on 6 December 1997, MAJ John Doe, Chief, Plans and Ops Division, reported that during a routine end-of-day check the previous afternoon he discovered a classified document left unsecured in room 215, bldg 2552. The document was found among a stack of unclassified documents left on the windowsill behind the desk occupied by CPT Smith. CPTs Smith and Jones occupy the office itself. MAJ Jones secured the all the document and subsequently released it to this office. (See MAJ Doe's statement at encl 1)

2. A review of the material disclosed that all documents, except one marked SECRET-RELROK, titled "War Strategies of Attilla the Hun", were unclassified. The unclassified documents were released to CPT Smith.

3. Further investigation revealed that CPT Smith left the office at approximately 1700 Hrs and secured the door to the room at that time. In addition, the investigation that the room is routinely left unlocked and unattended during duty hours. There are only three keys issued for the office, one to CPT Smith, one to CPT Jones, and one to the Chief, MAJ Doe. The master key is located in a locked classified container in the Division Admin office. MAJ Doe verified that the office was locked when he opened it at 1800 Hrs.

4. The document originated in the ACofS, C2 IP Division and a review of the document by the IP Division Chief, COL Jack Pratt determined that the document must remain classified and a compromise of the document would cause serious damage to the national security. (See COL Pratt's statement at Encl 2).

5. An interview with CPT Smith revealed that to the best of his recollection, he had neither seen, nor handled the document in question, and could not determine how long the document had been on his windowsill. The last time he sorted through the stack of files was in mid-November 1997. (See CPT Smith's statement at encl 3.)

6. Conclusion: Based on the interviews and the investigation conducted it is concluded that the probability of compromise is not remote. The document may have been unsecured for an extended period of time in an office that remains unlocked and often unattended during duty hours.

7. Recommendations:

a. CPT Smith receives a verbal reprimand.

b. That the office is secured when unattended.

c. That the required security checks are performed at the end of duty hours.

8. It is further recommended that the investigation is closed and an investigation under AR 15-6 is not required.

9. POC for the action is the undersigned at 723-0000.

CFCB-IS-S-IPS
SUBJECT: Preliminary Inquiry

Encl
As

JANE DOE
MAJ, AR
ACofS, C2

NOTE. In the event that the preliminary inquire could not identify a responsible individual further investigation under AR 15-6 may be recommended.