Department of the Army
Headquarters, U.S. Army Garrison
UNIT 17001, BLDG 730
APO, AP 96555
4 June 2025

Kwajalein Atoll Regulation 380-5

Command Security Program

Page Intentionally Left Blank

TABLE OF CONTENTS

Cover Page

Table of Contents

Chapter 1
General, page 1
Purpose ● 1-1, *page 1*
References ● 1-2, *page 1*
Terms & Definitions ● 1-3, *page 1*
Records management ● 1-4, *page 1*
Change management ● 1-5, *page 1*

Chapter 2 Responsibilities
USAG-KA Commander ● 2-1, *page 1*
Security Manager ● 2-2, *page 3*
Supervisors ● 2-3, *page 4*
All Army Personnel ● 2-4, *page 5*

Chapter 3 Policy
General ● 3-1, *page 5*
Implementation ● 3-2, *page 5*
Information Security ● 3-3, *page 8*
Emergency Action Plan ● 3-4, *page 11*
Personnel Security ● 3-5, *page 14*
Security Inspections ● 3-6, *page 15*
Visit Procedures ● 3-7, *page 15*
Operational Security ● 3-8, *page 16*

Appendixes:

A. References, *page 18*

B. Terms & Definitions, *page 19*

C. Emergency Action Plan, *page 23*

D. Courier Accountability & Safeguarding Procedures, *page 25*

E. Receipt/Courier Briefing, *page 26*

Chapter 1 General

1-1. Purpose
1. To establish uniform security policy and procedures for internal security functions for the US Army Garrison – Kwajalein Atoll (USAG-KA). To familiarize element personnel with applicable security requirements to ensure a sound security posture. This regulation will be used in conjunction with applicable security references and is applicable to all personnel assigned to USAG-KA.

1-2. References
See appendix A.

1-3. Terms
See appendix B.

1-4. Records management (recordkeeping) requirements
1. The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Records Retention Schedule-Army (RRS – A). Detailed information for all related record numbers, forms, and reports are located in the Army Records Information Management System (ARIMS)/RRS – A at https://www.arims.army.mil. If any record numbers, forms and reports are not current, addressed, and/or published correctly in ARIMS/RSA – A, see DA Pam 25 – 403 for guidance.

1-5. Change Management
1. Significant changes will require staffing and approval. When such changes are made the revision number will be incremented and the change number reset. Minor and/or administrative changes will not need re-approval and only the change number will be incremented.

2. Send comments or suggested improvements to the USAG-KA Installation Security Specialist via the command at Building 730, Kwajalein Atoll; 808-580-2110.

Chapter 2
Responsibilities

2-1. USAG Kwajalein Atoll Commander
1. Commanders at all levels and heads of agencies and activities are responsible for effective management of the information security program within commands, agencies, activities, or areas of responsibility (referred to within this regulation as commands). Commanders may delegate certain authorities to execute the requirements of this regulation, where applicable, but not their program management responsibilities. Security, including the safeguarding of classified and Controlled Unclassified Information (CUI) and the appropriate classification and declassification of information created by DA personnel, is the responsibility of the commander. The commander will—

a. Establish written local information security policies and procedures and an effective information security education program, consistent with this regulation.

b. Formulate and supervise measures or instructions necessary to ensure continuous protection of classified information, CUI, and related materials.

c. Ensure that persons requiring access to classified information have met the appropriate security clearance eligibility, access standards, and have a need-to-know.

d. Continually assess the individual trustworthiness of personnel who possess security clearance eligibility and who have been given access to classified information.

e. Designate a Security Manager (SM) in writing. Ensure the SM is of sufficient rank or grade to effectively discharge assigned duties and responsibilities.

f. Ensure the SM has been the subject of a favorably adjudicated, current background investigation appropriate for the highest level of classification of information and the appropriate access to the level of information managed.

g. Ensure the SM receives security training consistent with assigned duties and this regulation.

h. Ensure adequate funding and personnel are available to allow security management personnel to manage and administer applicable information security program requirements.

i. Review and inspect the effectiveness of the information security program within the Command annually or more frequently based on program needs and classification activity.

j. Ensure prompt and appropriate responses are given, or forwarded for higher echelon decision, to any problems, suggestions, requests, appeals, challenges, or complaints arising out of the implementation of this regulation.

k. Ensure the prompt and complete reporting of security incidents, violations, and compromises related to classified information or the unauthorized disclosure of CUI, as directed herein.

l. Ensure violations of this regulation, including suspected compromises or other threats to the safeguarding of classified information and the unauthorized disclosure of CUI, are reported and investigated IAW this regulation.

m.Ensure prompt reporting of credible derogatory information on assigned or attached personnel and contractors, to include recommendations for or against continued access to classified information IAW AR 380–49 and AR 380– 67.

n. Ensure compliance with the requirements of this regulation when access to classified information is provided to industry at a facility or location for which the

Command is responsible, in connection with a classified contract. If the classified information is provided to industry at the contractor's facility, ensure compliance with the provisions of AR 380–49.

o. Include the management of classified information as a critical element or item in personnel performance evaluations where appropriate, as directed in the provisions of EO 13526.

2-2. Security Manager

1. The SM is the principal advisor on information security in the Command and is responsible to the Commander for management of the program. The SM will have direct access to the Commander on matters affecting the information security program. The SM will—

a. Advise and represent the Commander on matters related to the classification, downgrading, declassification, and safeguarding of national security information.

b. Establish and implement an effective security education program for the Command as required by chapter 8 of AR 380-5.

c. Establish procedures for ensuring that DA personnel who handle classified material are properly cleared IAW AR 380–67.

d. Advise and assist officials on classification problems and the development of classification guidance.

e. Ensure that classification guides for classified plans, programs, projects, or mission are properly prepared, approved, distributed, and maintained.

f. Conduct a periodic review of classifications assigned within the activity, to ensure classification decisions are consistent with DOD classification guidelines.

g. Consistent with operational and statutory requirements, review classified and CUI documents in coordination with the Command Records Management Officer. Continually reduce, by declassification, destruction, or retirement, as appropriate, unneeded classified and CUI information and material.

h. Oversee or conduct security inspections and spot checks for compliance with this regulation and other security regulations referenced herein and directives and notify the Commander of the results.

i. Assist and advise the Commander in matters pertaining to the enforcement of regulations governing the access to, and the dissemination, reproduction, transmission, transportation, safeguarding, and destruction of classified or CUI information and material.

j. Make recommendations, based on applicable regulations, and directives, on requests for visits by foreign nationals and foreign government representatives. Provide security and disclosure guidance if the visit request is approved. For further guidance regarding official visits by foreign government representatives, refer to AR 380–10.

k. Ensure violations of this regulation, including suspected compromises or other threats to the safeguarding of classified information and the unauthorized disclosure of CUI, are reported and investigated IAW this regulation. Recommend appropriate corrective actions to address security violations.

l. Ensure proposed public releases concerning classified or sensitive programs are reviewed to preclude the release of classified information, CUI, or other sensitive unclassified information exempt from release under the Freedom of Information Act (FOIA).

m. Establish and maintain visitor control procedures in cases in which visitors are authorized access to classified information or to areas where classified material is stored and or processed.

n. Issue contingency plans for the emergency destruction of classified information and CUI, when necessary, and for the safeguarding of classified and CUI information used in or near hostile or potentially hostile areas.

o. Be the single point of contact to coordinate and resolve classification or declassification problems.

p. Report data as required by this regulation.

2-3. Supervisors

1. Supervisory personnel have a key role in the effective implementation of the command's information security program. Supervisors, by example, words, and deeds, set the tone for compliance by subordinate personnel with the requirements to properly safeguard, classify, and declassify information related to national security. Supervisors will—

a. Ensure subordinate personnel who require access to classified information are properly cleared IAW AR 380–67.

b. Ensure subordinate personnel are trained in, and comply with the requirements of this regulation, as well as local policy and procedures concerning the information security program.

c. Continually assess the eligibility of subordinate personnel for access to classified information, and report to the SM any information that may have a bearing on that eligibility IAW AR 380–67.

d. Include the management of classified information as a critical element or item in personnel performance evaluations, where appropriate.

2-4. All Army personnel

1. All DA personnel, regardless of rank, title, or position, have a personal, individual, and official responsibility to safeguard information related to national security they have access to. All DA personnel will report, to the proper authority, actions by others or any other matters that could lead to, or that have resulted in, the unauthorized disclosure or compromise of classified information or CUI.

Chapter 3 Policy

3-1. General

1. Security requirements established by the Commanding General, Installation Management Command (IMCOM) and implemented by USAG-KA consistent with applicable Army regulations, directives, and policy. The Garrison Security Manager will ensure all incoming classified documents are reviewed to ensure documents are properly marked, stored, and safeguarded.

3-2. Implementation

1. Storage and Retention.

a. All classified material, regardless of medium, will be stored in a security container when not in use. Supervisors will ensure personnel are properly cleared and have a need-to-know prior to granting access to a security container. On-site contractor personnel may have access to the security container as required if they have the appropriate security clearance and need-to-know. Contract safe custodians will ensure access by their on-site contractors is limited to only that information required in the performance of the contract. Contractors with knowledge of a security container combination will be included on item 10, SF 700; the contractor's telephone will be included to be contacted should the container be found unlocked and unattended. Security containers combinations will be maintained IAW AR 380-5.

b. USAG-KA and contractor safe custodians will change security container combinations within the U.S. Army Garrison Kwajalein Atoll consistent with requirements of AR 380-5.

c. Security containers no longer needed will be prepared for turn-in IAW AR 380-5. The combination will be reset to the standard 50-25-50, labeled with the combination and status and include opening instructions for non-standard locks.

d. Security containers will remain under constant surveillance when unlocked; the OPEN/LOCKED placard will be utilized. Appropriate entries will be made on the SF 702, Security Container Check Sheet each time the container is opened or closed. The end-of-day security check will be annotated on SF 701, Activity Security Checklist.

e. Classified documents no longer needed, will be destroyed. Custodians will continue to protect classified material identified for destruction until it is actually destroyed.

f. Working papers will be reviewed periodically by the originators for possible destruction. When maintained 180 days and beyond, the classified working papers will be marked, brought under control, and filed according to paragraph 5-20, AR 380-5.

g. Classified and CUI records should be maintained separately.

h. All government documents, both classified and Controlled Unclassified Information, will be destroyed IAW AR 380-5.

2. USAG-KA personnel will ensure reproduction of classified information is accomplished IAW AR 380-5.

3. Transmission of all classified transmission both incoming and outgoing, including courier transmission, will be processed through the USAG-KA base support contractor Document Control or according to local security procedures.

4. Couriers of all hand carried material will be prepared by the custodian IAW AR 380-5. (See Appendix E, Courier Accountability and Safeguarding Procedures).

a. In order to hand-carry classified materials aboard commercial aircraft, the courier must have in their possession written courier authorization orders prepared on command letterhead that include all data outlined in paragraph 7-13, AR 380-5.

b. A Courier Authorization Card (DD Form 2501) may be issued for frequent local couriers within the Kwajalein geographical area. Request for courier card will be made by memorandum from the supervisor to the Garrison Security Manager and will include the name and grade of the individual. The courier authorization card is not authorized for use to board commercial aircraft. CONUS and OCONUS hand carried procedures require a separate process.

c. A list of all classified information carried must be maintained by your organization until accountability requirements are reconciled.

5. Couriers will:

a. Be briefed on their responsibilities prior to hand carry of classified information.

b. Keep classified material in your personal possession at all times. Never read, display, or use the material in any manner during transport, or in any public place. Never leave classified material unattended in vehicles, car trunks, planes, hotel room, etc.

c. Make prior arrangements for proper storage at a U.S. Government or cleared contractor facility if your trip involves an overnight stop or arrival at your destination after duty hours.

d. When emergency situations arise while on travel and classified information is

involved, contact the local FBI. All requirements for classified hand carry OCONUS will be approved by the Garrison Security Manager only.

6. Classified Facsimile Transmissions/Telephone Discussions will be handled with concurrence of the Garrison Security Manager.

7. Controlled Unclassified Information with proper caveats will be transmitted with marking intact over unsecured facsimile equipment between U.S. Government and DOD contractor agencies only.

8. Personnel at USAG-KA will ensure their work areas, including desktops, tabletops, file cabinets, bookcases, etc. are free from clutter and papers prior to departure at the end of the day. End-of-day security checks reduce potential vulnerability of inadvertent co-mingling of classified and CUI.

9. The last person to leave the building is responsible for conducting end of day checks. Each office will maintain on file a double check roster designating the primary and alternate double checkers signed by the division chief. A copy should be given to each employee. The end-of-day double checkers will check, verify, and ensure that:

a. All desks, wastebaskets, and other surfaces are free of classified and/or sensitive materials.

b. All classified security containers are properly secured, and the SF 702 and the SF 700 are properly annotated.

c. All classified computer media is removed and properly stored to include Classified hard drives.

d. Classified copiers will be checked to ensure no classified material was left in the copier.

e. All electrical appliances are turned off.

f. All filing cabinets containing sensitive personnel data are locked.

10. Directors will ensure all technical documents, both classified and CUI, are marked by the originator to identify those that contain information for which dissemination is controlled by statute, DOD directive, or regulation.

11. Security for USAG-KA information systems are utilized IAW the accreditation document for the system. Information Systems Security Officers are responsible for ensuring AIS operations, including electronic mail (e-mail), are conducted IAW command policy and procedures and are approved for processing classified information.

12. All computer storage media will be affixed with the appropriate label or marked with the highest level of classified information stored on the media to include disks, zip drives, cassettes, videos, classified hard drives, etc. Accordingly, in an environment where

classified information is generated, CUI computer storage media will be labeled as such also.

13. Access Control regarding visitors, to include contractor personnel, will be monitored sufficiently to preclude unauthorized access to classified information and CUI. Contract monitors will ensure contractor operations are consistent with contract requirements and security requirements.

14. All Security violations will be reported immediately upon discovery through proper supervisory channels to the security office. The person discovering the violation will prepare a written statement immediately outlining the details of the incident.

3-3. Information Security

1. The Department of the Army Information Security Program is established to ensure that information classified under the authority of Executive Order 13256 is protected from unauthorized disclosure. The security of the U.S. depends a great deal on the proper safeguarding of the classified information. To that end, USAG-KA personnel are charged with the responsibility to properly safeguard classified information and or materials. AR 380-5 contains detailed security requirements to be followed by all Department of Army personnel.

a. Responsibilities. The USAG-KA Commander maintains the responsibilities for ensuring that a properly qualified security manager, top secret document custodian, physical security inspector, key and lock custodian, and sufficient alternates/assistants are appointed in writing.

(1) All management and supervisory personnel have the responsibility to ensure that DOD national security information under their control is properly safeguarded. Further, they are required to keep their staff informed on all new security changes and procedures.

(2) The overall safeguarding of sensitive and/or classified information/materials is the responsibility of each person who has knowledge of that information. It should be noted that security regulations do not guarantee protection and cannot be written to cover all situations. Basic security principles, common sense, and a logical interpretation of applicable regulations must be applied.

b. Classification Authority.

(1) Original authority. The Commander and Deputy Commander, USA IMCOM are delegated the authority for original classification of information as TOP SECRET, SECRET, and CONFIDENTIAL.

(2) Derivative classification. Derivative classification is a determination that information is in substance the same as information currently classified, and the application of the classification markings. Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information that is already classified, or those who apply markings IAW guidance from an original classification authority.

(3) In accordance with AR 380-5, paragraph 2-5, information taken from a document classified by multiple sources will identify the source document, its date, the classification authority, and the downgrading instructions. A list of all documents used to compile a document will be kept with the file copy.

c. Markings.

(1) The overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked with the highest classification of the material contained.

(2) All custodians are responsible to ensure that all classified material in their possession is properly marked IAW AR 380-5.

(3) If there is no back cover for a classified document, the overall classification of the document will be marked or stamped at the top and bottom of the back of the last sheet.

(4) File Folders or Group of Documents. IAW AR 380-5, file folders will be marked conspicuously with the highest classification and warning notices of all classified documents included therein. Appropriate cover sheets will be affixed to classified files/documents when removed from security containers.

(5) Electronically Transmitted Messages. The record copy of each electronically transmitted message shall be marked as required by AR 380-5.

d. Storage and Storage Equipment.

(1) Only GSA-approved security containers will be used for storage of classified information at all USAG-KA offices. Locking bar type containers with Sergeant Greenleaf model 8077A padlocks will not be used for storage of classified information unless it is secured inside a GSA approved vault.

(2) The Garrison Security Manager will inventory all security containers at USAG-KA and assign an administrative number. The Garrison Security Manager will maintain a record containing the location and administrative and property accountability numbers for all security containers. Acquisition of new security containers will be coordinated with the Garrison Security Manager who will assign an administrative number when the container is placed in use.

(3) Custodians of containers are responsible for ensuring that combinations are changed annually. Combinations will not be set in sequence of 5-10-15, etc., and will not be set on numbers relating to birthdays, anniversaries, telephone numbers, or other common or relative events.

(4) Custodians of containers will coordinate with the Garrison Security Manager for any work request to be done on any security containers before containers are called in for repair. The custodian will notify, in writing, the Garrison Security Manager of any

relocation of security containers. Classified material storage equipment that has been repaired will be inspected before being placed back in service. If the security container has been drilled, the Garrison Security Manager will recertify the container prior to any classified material being stored in it.

(5) Turn-in or Transfer of Security Equipment. The responsible organizational element will notify the Garrison Security Manager, in writing, when a container is no longer used to store classified information. The Garrison Security Manager will make a formal security check before turn-in of container.

(6) Standard Form 702, Security Container Check Sheet, and Standard Form 700, Security Container Information, will be removed once the container is cleared.

(7) A notation "NO CLASSIFIED MATERIAL STORED IN THIS CONTAINER" will be signed, dated, and affixed to the top drawer.

e. Transmission.

(1) Classified material shall not be hand-carried from USAG-KA unless there is neither time nor other means available to accomplish operational objectives. The Commander, USAG-KA and Garrison Security Manager are the only officials authorized to hand-carry classified material from USAG-KA aboard Air Mobility Command flights. Approval to hand-carry classified material aboard a commercial aircraft must be approved by the Commander, USAG-KA, and the Garrison Security Manager. Classified material will not be hand-carried on the Airline of the Marshall Islands flights.

(2) All couriers departing USAG-KA hand-carrying classified information will have a courier authorization letter in their possession. Couriers will provide the Garrison Security Manager a copy of travel authorization and coordinated preparation of the authorization letter. All couriers will receive a courier briefing from the Garrison Security Manager or representative and sign a Classified Document Briefing/Receipt attesting that they have read and understand applicable security directives.

(3) Whenever classified material is hand-carried between the islands of the Atoll, office supervisors will ensure there is a record of the material being hand-carried, and the material is enclosed in two opaque, sealed envelopes (the inner envelope marked with the classification) both bearing the return and destination addresses. Couriers must notify their office supervisor of any deviation from their schedule or return within a responsible period of time (determined by office supervisor). The Garrison Security Manager will be notified immediately of any deviation or delay.

(4) Offices transmitting classified material by mail will ensure the material is prepared IAW AR 380-5.

(5) Additionally, offices transmitting secret material are required to prepare receipts (Department of Army Form 3964) required by AR 380-5. If these receipts are not received within 30 days from the receiving office, the transmitting office will query them by submitting a tracer-action with the following comments in red: ‘‘TRACER

ACTION, REQUEST RESPONSE WITHIN 48 HOURS". An additional 15 days' suspense will be allowed. If no response is received or the receiving command denies receipt, the material will be traced through the postal system.

f. Reproduction.

(1) Top Secret material will not be reproduced without the consent of the originator or higher authority (AR 380-5 paragraph 7-3). Only the Top Secret Control Officer may destroy Top Secret material.

(2) All copies of classified documents reproduced are subject to the same controls prescribed for the document from which they were reproduced.

(3) Records will be maintained for two (2) years to show the number and distribution of all Top Secret documents, of all classified documents covered by special access programs distributed outside the originating agency, and all Secret and Confidential documents that are marked with special dissemination and reproduction limitations.

(4) The Garrison Security Manager will designate authorized copiers for the reproduction of classified material. All reproduction equipment within USAG-KA will be posted IAW AR 380-5.

g. Destruction.

(1) Classification documents and classified materials destroyed on USAG-KA will be accomplished by disintegration, burning, or shredding. Only those shredding machines that meet the specification of AR 380-5 will be used for shredding. Shredders must be approved by the Garrison Security Manager prior to their use for destruction of classified material. Office supervisors will ensure that all new destruction devices requisitioned by USAG-KA meet the specification of AR 380-5.

(2) All classified material once shredded will be taken to the island incinerator and burned. The destruction of Top Secret material requires records of destruction. The record shall be dated and signed at the time of destruction by the Top Secret Control Office and/or alternate plus one other witness who is cleared for access to Top Secret information. Department of Army Form 3964 will be used for this purpose.

(3) Classified material scheduled for destruction and classified waste such as handwritten notes, carbon paper, typewriter ribbons, and working papers, will be secured until such time that it can be properly destroyed. Classified waste will be disposed of as soon as possible and should under no circumstances be retained more than 30 days.

3-4. Emergency Action Plan (*See* Appendix C, Emergency Action Plan.).
1. Classified material will be protected during emergencies based on the existing threat.

a. Secure materials. Normally, employees will return all classified material to the security container and properly secure it.

b. In the case of fire or natural disaster, if circumstances warrant, employees may leave classified material in place during emergency evacuation to minimize the risk of injury or loss of life. All classified material will be accounted for upon return to preclude possible compromise. Should an explosion or natural disaster cause the shattering of classified materials, all available resources will be employed to provide retrieval and safeguarding as soon as conditions and circumstances allow.

2. Total destruction of classified material shall occur only at the direction of the USAG-KA Commander or Deputy to the Commander. In the event that destruction is ordered, material is prioritized for destruction as follows:

a. Priority One: Cryptographic/COMSEC keying material, i.e., microfiche, tape canisters, material.

(1) Destruction Method of Civil/Enemy: the COMSEC Hand Receipt Holder/Custodian will use a shredder, incendiary devices (outdoor use only), and/or a fire axe to destroy COMSEC keying material and COMSEC equipment.

(2) Destruction Method for Natural Disaster: COMSEC Hand Receipt Holder/Custodian will secure key material and/or equipment via GSA storage equipment.

b. Priority two: TOP SECRET, Sensitive Compartmented Information (SCI), North Atlantic Treaty Organization (NATO) COSMIC, and NATO COSMIC ATOMAL.

(1) Destruction Method for Civil/Enemy: Top Secret Custodian will use shredder or incendiary devices (outdoor use only). Record destruction of documents if possible.

(2) Destruction Method for Natural Disaster: Top Secret Custodian will secure classified material and/or equipment via GSA storage equipment and request assistance for placement of U.S. government personnel at safe zones of egress/ingress points in the building as feasible, to preclude unauthorized access or disclosure.

c. Priority three: U.S. SECRET, NATO SECRET ATOMAL, and NATO SECRET.

(1) Destruction Method for Civil/Enemy: Security Monitors/Document Custodians will secure classified material and/or equipment via GSA storage equipment and request assistance for placement of U.S. government personnel at safe zones at egress/ingress points of the building if feasible, to preclude unauthorized access or disclosure.

d. Priority four: U.S. CONFIDENTIAL, NATO CONFIDENTIAL ATOMAL, NATO CONFIDENTIAL, and NATO RESTRICTED.

(1) Destruction Method: Execute procedures in consonance with Priority Three above.

3. Supervisors will be knowledgeable of priority of material stored in their containers and will implement this plan during emergency evacuation. In situations not specifically anticipated by this plan, when warranted, the senior individual of an element may deviate from this plan utilizing basic security principles and guidelines IAW AR 380-5. Designated Command TOP SECRET Control Officers will utilize the Department of Army 3964 for the destruction of all TOP SECRET material. AR 380-40 Policy for Safeguarding and Controlling Communications Material contains policy for the emergency protection, including emergency destruction under no-notice conditions of COMSEC materials.

4. COMSEC Receipt Holders/Custodians will initiate "After Actions" destruction reports to their respective COMSEC Custodians.

5. Top Secret Custodians will initiate destruction reports for dissemination to higher headquarters and Department of the Army G-2, if required.

6. This Emergency Action Plan will be posted on or near each container or group of containers that store classified material.

7. After Action Requirements:

a. Conduct a sweep of the Special Compartmented Information Facility (SCIF) to assure that all materials have been destroyed, evacuated or secured.

b. Maintain the security of the SCIF until either the “all clear” or the evacuation is ordered.

c. After the “all clear” is announced develop a plan to restore operation of the SCIF.

d. If the determination is made to complete the evacuation/destruction of the rest of the material, it will be completed in an expeditious manner and the SCIF evacuated and secured.

e. Complete a post attack report which will include:

(1) Status of SCIF personnel,

(2) Percentage of material destroyed or evacuated,

(3) Present status of the SCIF, both equipment and facility status, and

(4) Requirements/recommendations/Comments.

3-5. Personnel Security

1. Personnel security is the application of standards and criteria to determine whether or not an individual is eligible for access to classified information, qualified for assignment or retention in sensitive duties, and suitable for acceptance and retention in the total Army consistent with national security interests.

2. Purpose:

a. To establish policies and procedures which ensure acceptance and retention of personnel in the Armed Forces, to include military, DOD civilians, DOD contractors, and other affiliated persons to receive access to classified information and or assignment to sensitive positions that are consistent with the interest of national security.

b. AR 380-67 is the primary source document used by USAG-KA and establishes DOD and Department of Army personnel security policies and procedures; sets standards, criteria, and guidelines upon which personnel security determination is based; prescribes the kinds and scopes of personnel security investigations required; details the evaluation and adverse action procedures by which personnel security determination shall be made; and assigns overall program management responsibilities.

3. Responsibility

a. The Garrison Security Manager has the primary responsibility for implementation of the command's personnel security program. Assistance in obtaining personnel security clearances, security briefings, security education, and control of classified visits to USAG-KA facilities are functions provided by the Security Manager. Contractors engaged in classified work and located at USAG-KA will establish and maintain their own personnel security program in compliance with AR 380-67.

b. Security criteria. The personnel security determination required by AR 380-67 is an overall, common-sense determination based on all available information. In arriving at the determination, certain activities and associations, current or past, of varying degrees of seriousness, warrant appropriate investigation and careful consideration. AR 380-67 provides detailed information concerning the standards for access to classified information or assignment to sensitive duties. The personnel security investigative requirements are covered in AR 380-67.

c. Requesting personnel security investigations. Requests for personnel security investigations shall be limited to those required to accomplish the defense mission. Such requests shall be submitted only by the authorities designated in AR 380-67. These authorities shall be held responsible for determining if persons under their jurisdiction require a personnel security investigation. Proper planning must be affected to ensure that investigative requests are submitted sufficiently in advance to allow completion of the investigation before the time needed to grant the required clearance or otherwise make the necessary personnel security determination. AR 380-67 amplifies the adjudication process in acquiring a personnel security clearance, and AR-380-67 also explains the process of granting and issuing personnel security clearances.

d. A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood of the individual preserving the national security. Obviously, it is not possible at a given point to establish with certainty that individuals will remain trustworthy. Accordingly, the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action.

3-6. Security Inspections

1. USAG-KA has security responsibility over the Garrison Sites within the Kwajalein Atoll.
2. All USAG-KA elements are required to undergo regularly scheduled command security inspections from United States Army Installation and Management Command (IMCOM). Inspections will be coordinated through the Commander, USAG-KA and will be announced or unannounced. Inspection reports will be provided to the USAG-KA Commander for action as they deem appropriate.

a. Security inspections performed as an integral part of the USAG-KA Command Inspection Program will follow appropriate regulations/directives.

b. The following is applicable to external security inspections or assistance visits:

(1) Specific inspection times and dates will be confirmed by inspecting personnel prior to scheduled inspection dates.

(2) Identification and security clearance of inspectors will be verified with Garrison Security Manager, extension 808-580-2110.

(3) The Garrison Security Manager or his designated representative will accompany the inspectors.

(4) An entry and exit brief will be presented to the principal staff officer or designated representative.

(5) The Garrison Security Manager will make available to the inspection team all applicable USAG-KA regulations.

(6) All correspondence relative to inspection results and or corrective actions taken will be sent to the Directorate of Plans, Training, Mobilization and Security.

3-7. Visit Procedures (See USAG-KA Regulation 190-10.)

1. Entry/Exit to USAG-KA. Entry authorization may be issued only after approval is given by duly authorized representatives of USAG-KA. Factors to be considered include:
a. (1) purpose of entry, (2) the possible burdens on logistics or threat to security and (3) facilities which the ship, aircraft or individual desires to visit. Requests for entry will be evaluated on a case-by-case basis.

2. Visit Authorization Requests. IAW AR 380-5, paragraph 5-14, DOD personnel visiting government activities of the DOD, its contractors, and other agencies shall provide advance notification of the pending visit that establishes the visitor's security clearance and the purpose of the visit. Visit authorization requests to another government installation or DOD contractor shall be accomplished using the Defense Information System for Security (DISS). DISS has been designated the system of record for all visit requests. Individuals who are slated to visit another installation off the USAG-KA will notify the Garrison Security Manager 14 days in advance of the requested visit. The following information is necessary to process a visit request to another installation:

a. Service Management Office Code (SMO) (e.g., Kwajalein's SMO code is W4T8AA6).

b. Purpose of the visit.

c. Point of Contact name and a telephone number at the visited site.

d. Start and End date of the visit.

3. If there will be a number of trips to the same installation over the course of the following year, indicate that and the visit will be good for a year.

a. In the rare instance that USAG-KA personnel are visiting an installation or contract facility that does not have access to DISS, personnel will use the most current USAG-KA Form 55R (USG Employee K-badge Form).

b. Contractor personnel visiting government or contractor facilities will comply with AR 380-67.

c. The visit will be signed by the Garrison Security Manager who is in a position to verify the visitor's security clearance. The USAG-KA Provost Marshal Office (PMO) is the central point for unofficial and foreign visitor incoming visit requests to Kwajalein Atoll. The PMO will forward copies to appropriate contractors listed on the visit request.

3-8. Operational Security

1. Operational Security (OPSEC) safeguards sensitive operations and activities on contracts and activities that are susceptible to hostile exploitation. Disclosure of these operations and activities could result in the compromise of current or future information. The traditional security program as directed by AR 381-10 which provides for countering the adversary intelligence threat by protecting classified information. In some cases, the protection of classified information has been inadequate for preventing combinations of Controlled Unclassified Information and stereotyped patterns from becoming OPSEC indicators (vulnerabilities), thus revealing sensitive aspects of a classified program, if not actual classified information. An active OPSEC program requires involvement by all elements associated with US Army operations. An active OPSEC program requires all elements, military, DOD civilians, and contractors, to continually evaluate each individual operation, activity, or project in light of all known adversary intelligence collection

methods, assess vulnerabilities, and establish measures to reduce or negate adversary intelligence collection capabilities.

2. The primary responsibility for establishing and maintaining the USAG-KA OPSEC program rests with the OPSEC manager. A local command OPSEC Standard Operating Procedures was published and distributed for the purpose of educating all personnel as to OPSEC responsibilities.

3. OPSEC is a continuous, systematic process that combines established security guidelines and common sense. It can be applied to any program, plan, or operation. The five fundamental steps in the OPSEC process are:

a. Determine critical information.

b. Analysis of threat.

c. Analysis of vulnerabilities.

d. Assessment of risk.

e. Application of countermeasures.

Each of these five fundamental steps incorporates many individual functional processes, or sub-steps.

CANNON.MATTHEW.JOHN.1247589801
Digitally signed by CANNON.MATTHEW.JOHN.1247589801
Date: 2025.08.09 17:09:51 +12'00'

MATTHEW J. CANNON
COL, AR (FA40)
Commanding

DISTRIBUTION:
All USAG-KA

The proponent element of this regulation is the Garrison Security Office. Users are invited to send comments to the Garrison Security Manager, Building 730, Room 127, APO, AP 96555.

This regulation supersedes USAG-KA/RTS Regulation 380-5, dated 09 February 2024.

APPENDIX A

References

Publications

AR 380-5, 25 March 2022
Army Information Security Program.

DoD Manual 5200.01, Volumes 1-3
DOD Information Security Program

AR 25-55, 19 October 2020
The Department of the Army Freedom of Information Act Program.

DoD Directive 5230.25, 6 November 1984, incorporating change 2, 15 October 2018
Withholding of Unclassified Technical Data from Public Disclosure.

Executive Order 13526, 29 December 2009
Classified National Security Information.

DoD Instruction 5230.24, 10 January 2023
Distribution Statements on DoD Technical Information.

AR 380-10, 14 July 2015
Foreign Disclosure and Contacts with Foreign Representatives.

AR 380-67, 27 March 2025
Personnel Security Program.

DoD Directive 5400.07, 5 April 2019
DOD Freedom of Information Act (FOIA) Program.

AR 381-10, 27 January 2023
The Conduct and Oversight of U.S. Army Intelligence Activities.

APPENDIX B

Terms & Definitions Access
The ability or opportunity to obtain knowledge of classified information.

Agency
In addition to the DODM 5200.01, Volume 1 definition, this term also includes the Army (an ACOM is not an agency, but rather is part of an agency, the Army). Within the Department of Defense (DOD), this term includes the DOD, the Department of the Army, the Department of the Navy, and the Department of the Air Force.

Code Word
A single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real–world military plans or operations classified as Confidential or higher.

Command
HQDA to include the Office of the Secretary of the Army and the Army Staff, ACOMs, ASCCs, DRUs, major subordinate commands and other organizations formed within the Army to support HQDA or an ACOM, ASCC or DRU.

Common access card
An identification card displaying the cardholder's name, photo, and organization. The CAC is the DOD implementation of Homeland Security Presidential Directive 12 that requires Federal Executive Departments and Agencies to implement a government-wide standard for secure and reliable forms of identification for employees and contractors, for access to Federal facilities and information systems and designates the major milestones for implementation.

Compromise
An unauthorized disclosure of classified information.

Continental United States
U.S. territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

Controlled Cryptographic Item
A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but controlled. (Equipment and components so designated bear the designator "Controlled Crypto-graphic Item" or CCI.)

Counterintelligence
Those activities which are concerned with identifying and counteracting the threat to security (of the Army and Government to include, but not limited to, its technology or industrial base) posed by foreign intelligence services or organizations, or by individuals engaged in espionage, sabotage, sedition, subversion, or terrorism.

Department of the Army personnel
Includes any Regular Army, U.S. Army Reserve, or ARNG/Army National Guard of the United States military personnel assigned or attached to a Department of the Army installation or activity, and civilian persons employed by, assigned to, or acting for an activity within the Department of the Army.

Event
An occurrence or happening that is reasonably certain to occur, and which can be set as the signal for automatic declassification of information.

Foreign Government representative
For the purposes of this regulation, foreign nationals or U.S. citizens or nationals who are acting as representatives of either a foreign government or a firm or person sponsored by a foreign government. These individuals may interact officially with DA elements only in support of an actual or potential U.S. Government program (for example, Foreign Military Sales, U.S. government contract, or international agreement).

Foreign Nationals
A person who is not a citizen or national of the U.S. or its territories. This definition does not include permanent residents (formerly immigrant aliens, resident aliens, or intending U.S. citizens). For the purposes of this regulation, a private non-U.S. citizen or national having no official affiliation with their government of origin. See definition of foreign government representative.

Information
Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of the U.S. Government.

Information System
An assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

Intelligence Activity
An activity that an agency within the intelligence community is authorized to conduct under EO 12333.

Loss
The inability to physically locate or account for classified information.

Mandatory declassification review
Review for declassification of classified information in response to a request for declassification that meets the requirements under EO 13526, Section 3.5.

Open storage
An area constructed IAW this regulation and authorized by the commander or other official where so designated for open storage of classified information.

Operations security
The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conducting of military operations and other activities.

Original classification authority
In addition to the DODM 5200.01, Volume 3 definition, this term also includes: An individual's position, which has been authorized in writing, either by the President, Secretary of the Army, or the DCS, G–2 to originally classify information up to and including a certain classification level.

Personal identifier
Any grouping of letters or numbers, used in an organization code, that the command uses to identify a position.

Security educator
Person(s) responsible for providing security training as outlined in chapter 8 of this regulation.

Security–in–depth
In addition to the DODM 5200.01, Volume 3 definition, this term also includes: A determination by the commander or other official where so designated, that a facility's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System, random guard patrols throughout the facility especially during nonworking hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of unalarmed open storage areas and security containers during nonworking hours.

Senior agency official
In addition to the DODM 5200.01, Volume 3 definition, this term also includes: Within the Department of the Army, the Secretary of the Army has appointed the DCS, G–2 as the Senior Agency Official.

Sensitive Information
Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an executive order or an Act of Congress to be kept Secret in the interest of national defense or foreign policy.

Source Document
An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Systematic Declassification Review
The review process for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value IAW chapter 33 of title 44, United State Code, 44 USC Chapter 33.

Technical counterintelligence (TEMPEST) countermeasures
Any action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment or facility that electronically processes information for technical exploitation of classified and/or sensitive information.

Telecommunications
The preparation, transmission, or communication of information by electronic means.

TEMPEST
A short name referring to the evaluation and control of compromising emanations from telecommunications and automated information systems equipment. TEMPEST countermeasures are designed to prevent Foreign Intelligence Service exploitation of compromising emanations by containing them within the IS of the equipment or facility processing classified information.

APPENDIX C

Emergency Action Plan (EAP). The EAP establishes policies and procedures for the safeguarding and/or destruction of classified material in the USAG-KA Secure Room(s), to include Communications Security (COMSEC) and collateral information.

1. During an emergency the security of classified material is secondary only to the safety of personnel. The Security Manager, acting on behalf of the USAG-KA Commander will review and approve this plan, and thereafter, will annually review and approve this plan as necessary. Updates to this plan, and recommendations for changes may be submitted at any time to the Security Manager USAG-KA, APO, AP 96555. This plan is not all encompassing and is meant as a guide.

2. All personnel assigned to operate within the USAG-KA Secure room(s), will be familiar with this plan. All personnel are responsible for advising the safety of visitors during an emergency or implementation of this EAP.

3. The safeguarding and/or destruction of classified material in the USAG-KA Secure Room(s) will be determined by severity of events. Due to the remoteness of USAG-KA, the destruction of classified materials is unlikely, however, if time and circumstances permit, and the USAG-KA Security Manager believes destruction of classified materials is warranted the classified document emergency plan will be utilized.

4. Priority of Safeguarding and/or Destruction - Materials are identified for safeguarding and/or destruction as follows:

a. Priority One: All cryptographic equipment and documents.

b. Priority Two: All sensitive intelligence materials and TOP SECRET collateral.

c. Priority Three: SECRET and Confidential classified material. Only the minimum number of classified materials required to perform one's duties should be removed from containers. In the event of an emergency, the material can be quickly gathered and returned to or placed into a locked container. Absent the Security Manager, the most senior individual is responsible for securing the Secure Room(s) upon evacuation.

5. Emergency Destruction Procedures.

a. If required, documents will be burned and/or shredded. If the documents are burned, the ashes will be sifted.

b. If required, CD/DVD will be burned (time permitting). If unable to burn, CD/DVD will be scored and broken in pieces.

c. If required, equipment will be smashed with a hammer or other implement. Like equipment should be damaged in the same part of like equipment. This will prevent anyone from cannibalizing one piece of equipment to fix another piece of equipment.

6. Fire Protection. Natural or man-made fires may occur with little or no warning. (A fire equipment diagram, showing locations of pull boxes, fire extinguishers, hoses, escape routes, etc., needs to be included in the EAP).

7. Bomb Threat. In the event of a bomb threat, DO NOT HANG UP! Utilize Form FD-730 (5-6-87) or a similar form. Try to alert a second worker to contact security to trace the call and initiate an evacuation of the building and Secure Room(s). (Keep in mind some bombers may plant a secondary device in the evacuation area or plant the primary device in the evacuation area. Therefore, more than one area should be established.)

8. Natural Disasters. The most significant natural disasters that may occur are heavy rain and inundation events.

9. Sabotage or Terrorist Attack. The possibility of such an attack is remote.

10. Riots or Civil Disorders. The possibility of such an occurrence is remote.

11. Loss of Utilities. In the event of loss of electrical power, the battery back-up for the Intrusion Detection System will automatically activate. However, as no windows are available to provide natural light, the Secure Room(s) may be secured by placing a cleared individual outside of the entrance. Posting personnel on the door will continue until electrical power is operational.

12. Aircraft or Rocket/Missile Incident. The most probable cause of an incident may be either an aircraft mishap (either an accident or planned) or an errant rocket/missile, with devastating results occurring quickly and without warning. In the event of a fire, the fire department is in charge regardless of the cause. However, once the fire is terminated, the on-scene fire commander relinquishes command to law enforcement if criminal activity is suspected or to another agency. The Security Manager or senior representative must make their presence and responsibility known and work with the on-site commander.

13. Admittance of Emergency Response Personnel and Their Equipment. Admittance of Emergency Response Personnel (i.e. fire, ambulance, and police) and their equipment will be permitted without delay. Personnel will be identified when able and available and will be asked to sign a non- disclosure agreement when the emergency is terminated. Personnel should power down their systems and if unable, at a minimum, turn off their computer screens and terminate any classified conversations. The use of transmitters by emergency response personnel inside the Secure Room(s), during an emergency is permitted.

APPENDIX D

Courier Accountability and Safeguarding Procedures. All personnel who regularly hand carry classified information locally will be issued a DD Form 2501, Courier Authorization Card. Such persons will use the courier card to identify themselves to any inspector as a properly authorized courier of classified information. It is valid only within the local geographic area to include USAG-KA controlled islands. The Courier Card will not be used as authorization to hand carry classified material outside the local area, TDY, or aboard commercial aircraft. AR 380-5 outlines the hand carrying of classified material off the installation.

1. The DD Form 2501 is a controlled item managed by the Security Manager's Office.

a. The Garrison Security Manager will issue courier cards to USAG-KA personnel in serial number blocks.

b. Cards will be issued to cleared employees who regularly hand carry classified information locally. Regularly in this case is defined as a need to hand carry at least once a week.

c. The DD 2501 is valid for one year from date of issue and must be renewed annually.

d. The card must be terminated when an employee leaves government service, transfers to another organization, or when the card is lost or no longer required.

e. USAG-KA issue and accountability procedures.

2. DD Forms 2501 will be issued only by the Security Manager or his/her designated security personnel.

3. The Security Manager or his/her designated security personnel will maintain accountability of DD Forms 2501 issued within USAG-KA. A written log will be maintained specifying status of each courier card (issued (to whom), on hand/not issued, lost or destroyed).

4. Individuals issued DD Forms 2501 will acknowledge receipt of the courier card and the courier briefing (see enclosure 1). The Security Manager will retain the receipt as long as the card is valid. When a new card is issued, the individual will again receipt for the card and receive a new briefing.

5. An individual who no longer required a DD Form 2501 will return the card to the Security Manager's office.

6. The Security Manager will destroy all DD Forms 2501 that are no longer valid (expired, employee transferred, no longer required, etc.).

7. The Security Manager will safeguard unissued DD Forms 2501 in a security container.

DD FORM 2501
RECEIPT/COURIER BRIEFING

(Office Symbol) (Date)

I, the undersigned, acknowledge receipt of DD Form 2501, and confirm that I have received the courier briefing.

(Signature of Courier)

(Signed copy retained by Security Manager's Office)

(Instructional copy retained by individual)

1. As a courier of classified information, I acknowledge that I am responsible for ensuring the integrity of the material at all times, specifically:

a. I will keep the material in my personal possession at all times.

b. I will not read, display, or use the material in any manner during transport.

c. I will not keep classified information overnight.

d. I will use the most direct route to my destination.

e. I will immediately report security incidents to the Security Manager's Office.

2. I am required to have in my possession an identification card or picture security badge, and written authorization to carry classified information, e.g., DD Form 2501 or other authorization.

3. I understand that the DD Form 2501 is valid for local hand carries only. AR 380-5 outlines the hand carrying of classified information off the installation.