Headquarters, United States Marine Corps

Guide to Security

Administration & Resource Management Division

Security Programs & Information Management Branch

The Security Programs and Information Management Branch (ARS) provides Information, Personnel, Physical and Communications Security services in support of HQMC Staff Agencies. These services also include security related training for all Marines/ Civilian Marines and contractors assigned to HQMC. The purpose of this Layman's guide is to familiarize you with some of the more common areas of the HQMC Security Program that affect the operation of your Staff Agency, department, or activity on a daily basis. Within this guide is the new Security Services Form. This form should be used to request most of the security related services found in this guide. However, as always we will respond to urgent request by any available media. The Security Services Form also contains a customer satisfaction rating and comments section, to let us know what we are doing and how we can do it better. Although not all encompassing, we feel you will have a better understanding of how to receive security related services and support. We encourage your comments and recommendations to assist us in better serving you.

A. A. WASHINGTON
Director, of
Administration and Resource
Management Division

Note: This document may be found at:
http://hqinet001.hqmc.usmc.mil/marinesecurity/index.htm

Table of Contents

Security Services Form 3

DoD Badges 4

Parking 5

Courier Cards 6

Check-in/Check-out Procedures 7

Security Manager's Notes 8

Mailouts 9

Information Personnel Security Program (IPSP) 10
Staff Assist Visits

Unannounced Security Visits (USV) 11

Working Papers 12

Reproduction 13

Marking 14

Communications Security 15

HQMC Physical Security 16

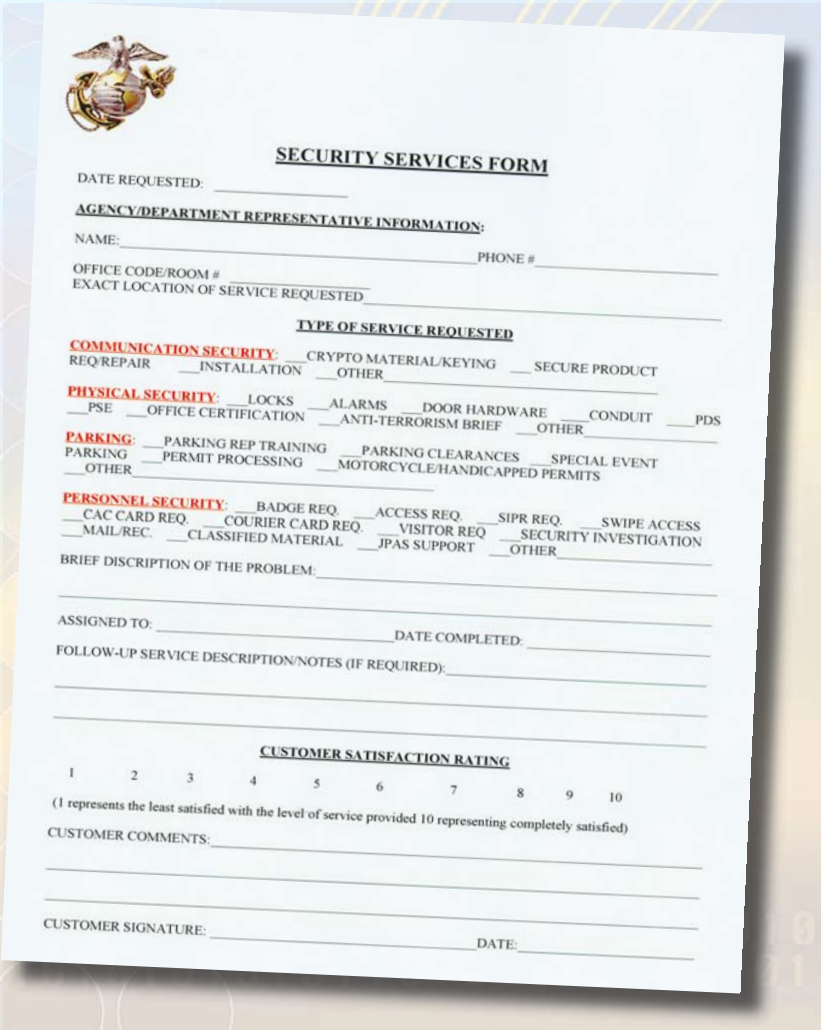
Security Training 17

Force Protection Conditions 18

Security Violations 19

Security Services Form

The Security Services form is the method in which certain security related services are requested. This form can be found at: ***http://hqinet001.hqmc.usmc.mil/marinesecurity/index.htm***



SECURITY SERVICES FORM

DATE REQUESTED: _____

AGENCY/DEPARTMENT REPRESENTATIVE INFORMATION:

NAME: _____ PHONE # _____

OFFICE CODE/ROOM # _____

EXACT LOCATION OF SERVICE REQUESTED _____

TYPE OF SERVICE REQUESTED

COMMUNICATION SECURITY: ___CRYPTO MATERIAL/KEYING ___ SECURE PRODUCT REQ/REPAIR ___INSTALLATION ___OTHER _____

PHYSICAL SECURITY: ___LOCKS ___ALARMS ___DOOR HARDWARE ___CONDUIT ___PDS ___PSE ___OFFICE CERTIFICATION ___ANTI-TERRORISM BRIEF ___OTHER _____

PARKING: ___PARKING REP TRAINING ___PARKING CLEARANCES ___SPECIAL EVENT PARKING ___PERMIT PROCESSING ___MOTORCYCLE/HANDICAPPED PERMITS ___OTHER _____

PERSONNEL SECURITY: ___BADGE REQ. ___ACCESS REQ. ___SIPR REQ. ___SWIPE ACCESS ___CAC CARD REQ. ___COURIER CARD REQ. ___VISITOR REQ ___SECURITY INVESTIGATION ___MAIL/REC. ___CLASSIFIED MATERIAL ___JPAS SUPPORT ___OTHER _____

BRIEF DISCRIPTION OF THE PROBLEM: _____

ASSIGNED TO: _____ DATE COMPLETED: _____

FOLLOW-UP SERVICE DESCRIPTION/NOTES (IF REQUIRED): _____

CUSTOMER SATISFACTION RATING

1 2 3 4 5 6 7 8 9 10

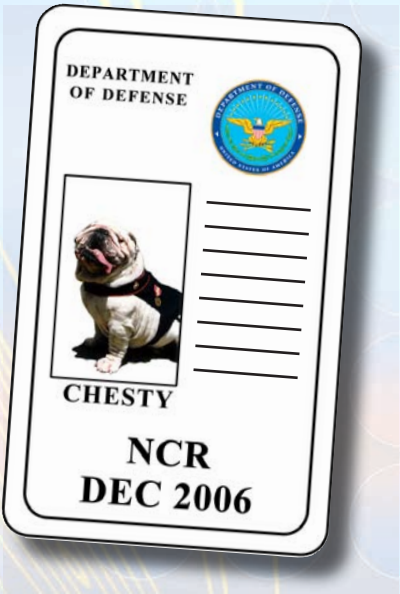
(1 represents the least satisfied with the level of service provided 10 representing completely satisfied)

CUSTOMER COMMENTS: _____

CUSTOMER SIGNATURE: _____ DATE: _____

DoD Badges

Agency Security Coordinators are required to provide their personnel with a badge request form for submission to ARS for processing. ARS is located in the Navy Annex, Room 1006. ARS will provide the individual with a DD 2249 form to take to the Pentagon Badge Office located at the Navy Annex or Pentagon. DoD, military, civilians, and contractors must have a completed investigation or NCIC to obtain a DoD badge. National Capital Region badges must have sufficient written justification to warrant the issue of a NCR Badge (access to multiple buildings is not Sufficient justification to obtain a NCR badge).



General Officers/Senior Executive Service Members, Executive Assistants, and Deputy Directors are automatically authorized NCR Badges. Security Coordinators are encouraged to coordinate with ARS to expedite the handling of General Officers/Senior Executive Service Members prior to issuance.

For questions please contact the Security Helpdesk at (703) 614-2320.

Parking

All Executive, “A”, “A” Numbered, and “C” permits are managed by the HQMC Parking Control Officer.

Staff Agency Parking Reps are responsible for processing parking permit applications for their respective agencies.

Permanent handicapped “H”, Carpool, Motorcycle and Vanpool permits are the responsibility of the Pentagon Parking Management Office. You may apply for one of these permits by contacting the Pentagon Parking Management Office at (703) 697-6251.

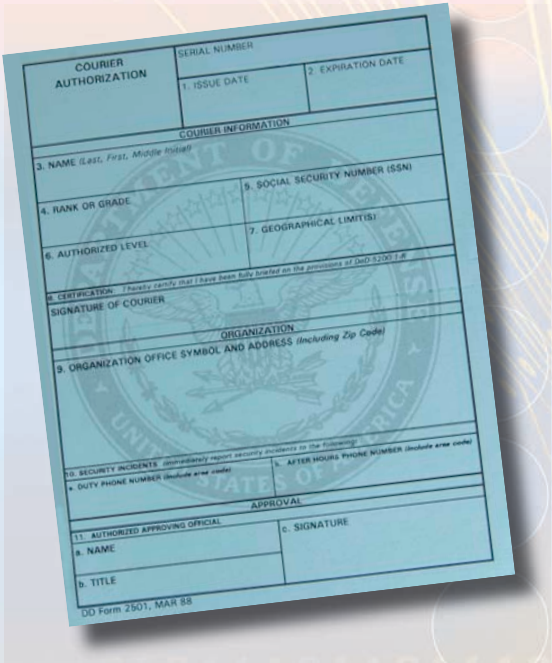
All VIP and visitor parking requests must be submitted to the HQMC ARS org mail box (below) 24 hours in advance of the visit.

The HQMC Parking Control Officer is located in Room 1012 Navy Annex, and can be reached by phone at (703) 695-0570.
E-mail address: SMB_HQMC_ARS_PARKING@usmc.mil

Courier Cards

All personnel that transport classified material, regardless of destination (outside of the Pentagon or Navy Annex) must be in possession of a Courier Card. Courier Cards may be obtained by contacting ARS. A letter from the Security Coordinator must be hand carried to ARS by the individual. ARS will then verify the individuals access to classified material and prepare the courier card at that time. All personnel must sign for their own Courier Card.

For questions please contact the Security Helpdesk at (703) 614-2320.


COURIER AUTHORIZATION
SERIAL NUMBER
1. ISSUE DATE
2. EXPIRATION DATE
COURIER INFORMATION
3. NAME (Last, First, Middle Initial)
4. RANK OR GRADE
5. SOCIAL SECURITY NUMBER (SSN)
6. AUTHORIZED LEVEL
7. GEOGRAPHICAL LIMITS)
8. CERTIFICATION I hereby certify that I have been fully briefed on the provisions of DoD 5200.1-R
SIGNATURE OF COURIER
ORGANIZATION
9. ORGANIZATION OFFICE SYMBOL AND ADDRESS (Including Zip Code)
10. SECURITY INCIDENTS (Immediately report security incidents to the following)
a. DUTY PHONE NUMBER (Include area code)
b. AFTER HOURS PHONE NUMBER (Include area code)
APPROVAL
11. AUTHORIZED APPROVING OFFICIAL
a. NAME
b. TITLE
c. SIGNATURE
DD Form 2501, MAR 88

Check-In/Out Procedures

ARS, Room 1006, Navy Annex

All personnel checking into HQMC must check into ARS with the required forms listed below. Personnel will receive the required forms from their Agency Security Coordinator.

- NAVMC 512 (Classified Information Access Authorization) is used to initiate and document an individual's authorization to handle classified information at Headquarters Marine Corps.
- SF312 (Non Disclosure Agreement).
- Badge request form.
- DD 2875 (if SIPRNET is required).
- Courier Card letter (if courier card is required).

It is mandatory that all personnel check out with ARS. This is required to prevent anyone from gaining access to classified material if they do not have a need-to-know. The following list of items must be turned into ARS. Please ensure all personnel checkout with ARS on their LAST DAY.

- DOD Badge turn-in
- Courier Card turn-in
- Parking Permit turn-in
- Blue Key

For questions please contact the Security Helpdesk at (703) 614-2320.

Security Manager's Notes

Security Manager's Notes provide local Security Policy Guidance information specific to HQMC.

The information contained within these notes are directive in nature when signed by the Dir,AR, Dep Dir AR, or HD ARS. Security Manager Notes can be found at:

http://hqinet001.hqmc.usmc.mil/marinesecurity/index.htm

For questions please contact the Security Helpdesk at (703) 614-2320.

Mailouts

All HQMC Staff Agencies located in the National Capital Region (NCR) that mail classified information must use the mailing services provided by the HQMC, Information Security Specialist, room 1006, Federal Office Building 2 (FOB2).

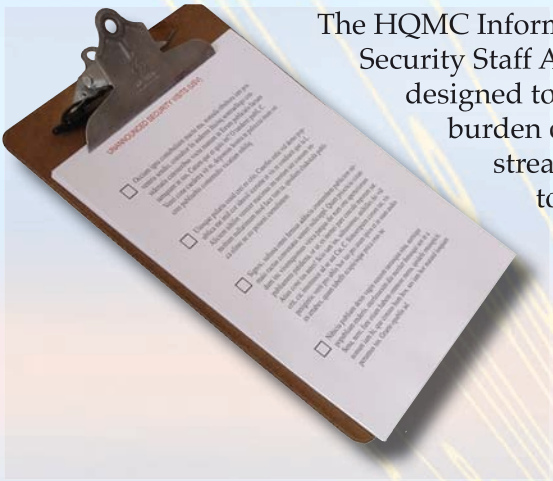
All classified documents/material being mailed by the HQMC Information Security Specialist must be sent Registered Mail through the U.S. Postal Service.

Agencies may request mail out services via the HQMC Security Services Request Form.

For questions please contact the Security Helpdesk at (703) 614-2320.

IPSP

Information and Personnel Security Program (IPSP) Staff Assist Visit (SAV)



The HQMC Information and Personnel Security Staff Assist Visit Program is designed to reduce the administrative burden of inspections and streamline the process of review to ensure compliance with Department of Defense and Department of the Navy regulatory requirements.

The IPSP Assist Visit Program is Announced annually in a Security Manager's Note. An outline is included in the Security Manager's Note identifying the areas that will be reviewed.

Two day advance notice of the IPSP Assist Visit will be sent via e-mail to the Security Coordinators and Assistant Security Coordinators.

For questions please contact the Security Helpdesk at (703) 614-2320.

USV

Unannounced Security Visits (USV)

The USV is a valuable tool in mitigating the loss and risk associated with the storage and handling of classified material. As a security awareness tool, USV's are intended to reduce the number of security violations within HQMC Staff Agencies.

USVs are conducted during normal working hours.

The checklist for the USV is provided annually in a Security Manager's Note.

For questions please contact the Security Helpdesk at (703) 614-2320.

Working Papers

Secret and Confidential working papers such as classified notes, research notes, rough drafts, and similar items that contain Secret or Confidential information shall be:

- Dated when created;
- Conspicuously marked centered top and bottom of each page with the highest overall classification level of any information they contain along with the words **"Working Papers"** on the top left of the first page in letter larger than the text;
- Protected per the assigned classification level; and
- Destroyed when no longer needed.

Agency's shall establish procedures to control and mark Secret and Confidential working papers in the manner prescribed for a finished document when retained more than 180 days from the date of creation or officially released outside the organization by the originator. A document transmitted over a classified IT System is considered a finished document.

For questions, please contact the Security Helpdesk at (703) 614-2320.

Reproduction

Classified information shall be reproduced only to the extent required by operational necessity unless restricted by the originating agency or for compliance with applicable statues or directives. Reproduction shall be accomplished by authorized persons knowledgeable of the Procedures for classified reproduction.

For questions, please contact the Security Helpdesk at (703) 614-2320.

Agencies Shall:

- Designate specific equipment for classified reproduction
- Ensure that all copies are subject to the same controls as the original information
- Limit reproduction to that which is mission-essential and ensure that appropriate countermeasures are taken to negate or minimize risk.
- Comply with reproduction limitations placed on Classified information by originators and special controls applicable to
- Special types of classified information
- Facilitate oversignt and control of reproduction

For questions please contact the Security Helpdesk at 703-614-2320.

Marking

All classified information shall be marked with the date and office of origin, the appropriate classification level and all required “associated markings”.

Marking is required on all information technology systems and electronic media, including removable components that contain classified information.

The proper marking of a classified document is the specific responsibility of the original or derivative classifier. While markings on classified documents are intended primarily to alert holders that classified information is contained in a document, they also serve to warn holders of special access, control or safeguarding requirements.

For questions please contact the Security Helpdesk at (703) 614-2320.

Communications Security

The HQMC Electronic Key Management Systems (EKMS) Manager is your sole source for all Communications Security (COMSEC) material and equipment. The EKMS 1 Manual and the HQMC COMSEC SOP provides minimum policy and procedures for the proper ordering, filling, generation, distribution, accountability, storage, usage, destruction, and management of COMSEC material/equipment.

The HQMC EKMS Section provides the following services:

- Key Management support.
- Secure Telephone support.
- Accounting, ordering, filling, distribution, storage, usage, and destruction, and management of electronic key and other types of COMSEC material.
- Policy and directive guidance.

All communications security related support may be obtained by contacting (703) 614-2305.

HQMC Physical Security

The HQMC Physical Security Manager is responsible for all HQMC Physical Security matters within the National Capital Region (NCR).

The HQMC Physical Security Manager provides:

- Physical Security Surveys.
- Restricted Area Accreditations.
- Security guidance for NCR renovations and new construction.
- Alarm system support.
- Access control requirements.
- Key and lock program support.
- Emergency lockout support (Doors & Safes).
- Foreign travel/country specific briefs.

The HQMC Physical Security Manager is located in room 1010 in the Navy Annex and can be reached by phone at (703) 614-4373.

Security Training

Security Training is an Annual Training requirement as outlined in SECNAV M-5510.30. This training package can be found at: ***http://hqiisdev001.hqmc.usmc.mil/marine%20security/launchPage.htm***

The online training consists of:

- Security Orientation/Refresher Brief
- Antiterrorism/Force Protection Brief
- Counterespionage Brief

***This training must be completed annually and Security Coordinators should ensure that completed rosters are provided to the ARS Security Office.**

Additional information is provided below to assist you with your agency/activity security program:

The Electronic Questionnaires for Investigations Processing System (e-QIP) is part of an e-government initiative sponsored by the Office of Personnel Management. e-QIP allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency for review and approval. The following link is a handbook for e-QIP usage from a Security Specialists perspective:
http://www.navysecurity.navy.mil/documents/jpas/eqip-manual.pdf

The following is a handbook for e-QIP Applicants. This handbook is for personnel who are filling out the security questionnaire:
http://www.navysecurity.navy.mil/documents/jpas/E-QIP%20Applicant%20Feb%202007.pdf

JPAS is the Joint Personnel Adjudication System. JPAS provides "real-time" information regarding clearance, access and investigative status to authorized DoD security personnel and other interfacing organizations. The following is a step-by-step color guide for JPAS usage:
http://www.navysecurity.navy.mil/documents/jpas/jpas-manual.pdf

For questions please contact the Security Helpdesk at (703) 614-2320.

Force Protection Conditions (FPCONs)

U. S. Northern Command assigns the FPCON's for the National Capital Region (NCR) via the Pentagon Force Protection Agency (PFPA). For current FPCON's go to ***www.pfpa.mil***

NORMAL Applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

ALPHA Applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable.

BRAVO Applies when an increased or more predictable threat of terrorist activity exists.

CHARLIE Applies when an incident occurs or when intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely.

DELTA Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent.

The Department of Homeland Security (DHS) provides the National Threat Advisory using the following chart.

For questions, please contact the PFPA Command Center at (703) 697-1001.

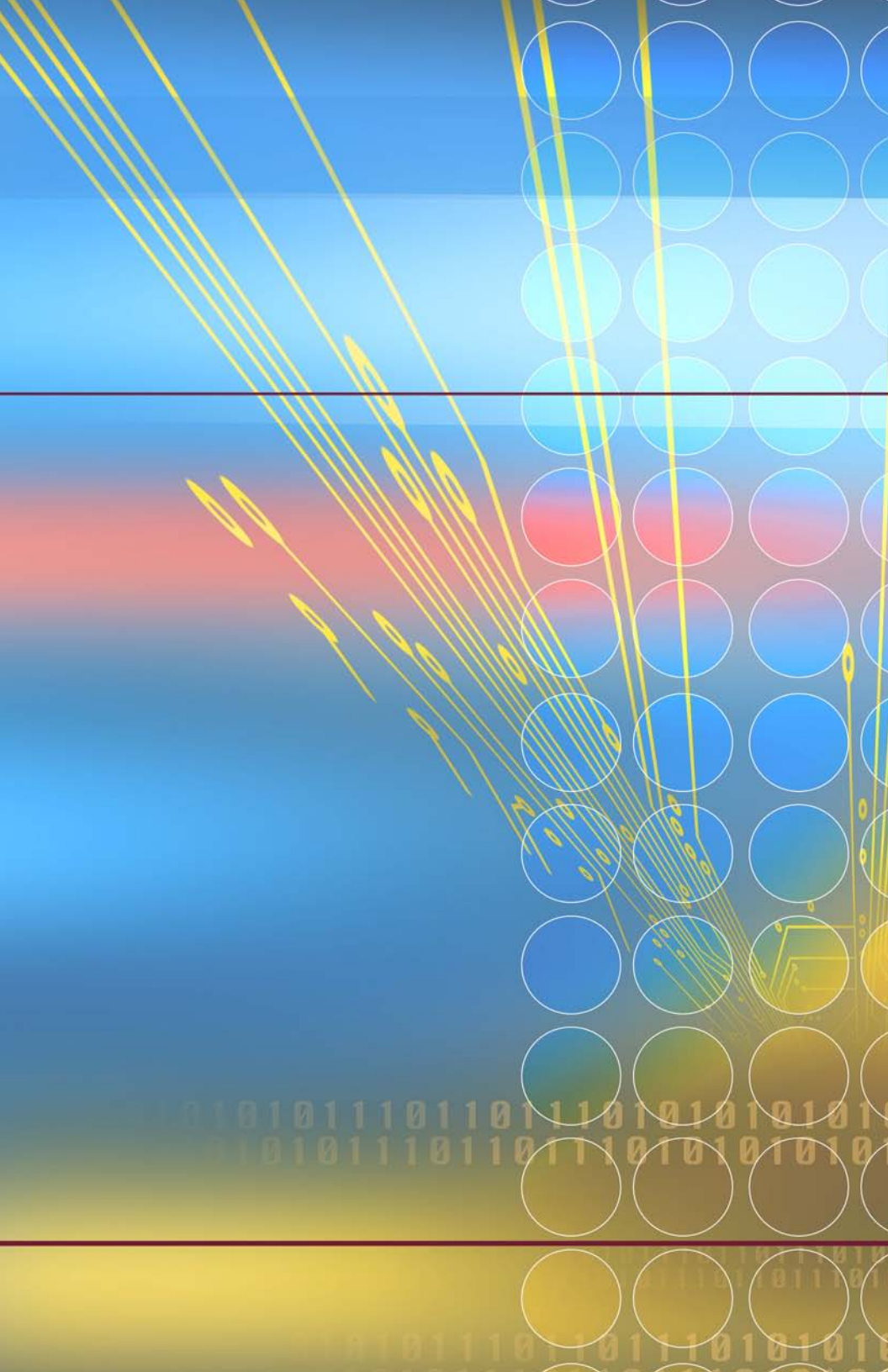
Security Violations

A security violation is the possible loss or compromise of classified information/material someone is entrusted to protect.

The following are common security violations throughout Headquarters:

- Unsecured Level III restricted areas.
- Classified documents sent via unclassified FAX.
- Classified documents sent via unclassified LAN.
- Classified material sent via guardmail.
- Improper mailouts.
- Unauthorized extension of a cryptoperiod.
- Use of COMSEC equipment or devices not approved by NSA.
- Improper use and employment of COMSEC equipment and devices via non-secure methods.
- Known or suspected espionage.

Report all security compromises/violations to the agency/department/activity Security Coordinator or directly to the HQMC Security Officer at 614-2320/3609.

Notes:

Notes: