



UNITED STATES MARINE CORPS
MARINE FORCES RESERVE
MARINE FORCES NORTH
2000 OPELOUSAS AVENUE
NEW ORLEANS, LA 70114-1500

ForO 5510.1A
Scty
JAN 09 2015

FORCE ORDER 5510.1A

From: Commander
To: Distribution List
Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)
Ref: (a) SECNAV M-5510.30B
(b) SECNAV M-5510.36
(c) NAVMC DIR 5040.6H
(d) MCO P5510.18A
(e) MCO 5530.14

Encl: (1) Information and Personnel Security Program Standard
Operating Procedures (IPSP SOP)

1. Situation. To publish procedures for the Information and Personnel Security Program (IPSP) within Marine Forces Reserve (MARFORRES) Headquarters (HQ) and the MARFORRES Major Subordinate Commands (MSC), and Marine Forces North (MARFORNORTH).
2. Cancellation. ForO P5510.1, ForO 5510.3, and ForO 5511.2.
3. Mission. MARFORRES HQs and the MSCs will ensure compliance with the provisions of this Order and the references as it pertains to the IPSP. "Commanding Officer" is used throughout this Standard Operating Procedures (SOP) as a generic term for the head of an organizational entity and includes Commander, Commanding General, Commanding Officer, Director, and Officer-in-Charge. The Commander, MARFORRES (COMMARFORRES) has overall responsibility for the IPSP for MARFORRES Commands and Staff Sections. This authority is delegated to the MARFORRES Command Security Manager and Deputy Command Security Manager as the responsible officer and subject matter expert.
4. Execution
 - a. Commander's Intent and Concept of Operations

(1) Commander's Intent

DISTRIBUTION STATEMENT A: Approved for public release;
distribution is unlimited.

(a) The references are the basic directives governing the IPSP within the Department of the Navy and the Marine Corps. The references supplement and incorporate the policy and guidance set forth in the Department of Defense (DoD) Personnel Security Program (DoD 5200.1) and DoD Information Security Program (DoD 5200.2).

(b) This Order implements the applicable provisions of the references and other pertinent directives as indicated in enclosure (1).

(c) Appendices A and B are lists of additional references and abbreviations used throughout enclosure (1).

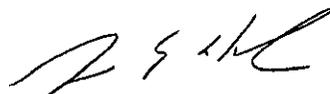
(2) Concept of Operations. The provisions of this Order are regulatory in nature and apply to all military and civilian personnel within this command without further implementation. A violation of these provisions by military personnel is punishable in accordance with the Uniform Code of Military Justice and could also be the basis for other administrative action or separation proceedings. A violation by civil service or contractor personnel may be cause for administrative disciplinary action that could result in dismissal.

5. Administration and Logistics. If guidance on a particular matter cannot be found in this Order or identified references, contact the appropriate MSC Security Manager or the MARFORRES Command Security Manager.

6. Command and Signal

a. Command. This Order is applicable to MARFORRES, and MARFORNORTH.

b. Signal. This Order is effective the date signed.



G. T. HABEL
Executive Director

DISTRIBUTION: C, D

Directives issued by this Headquarters are published and distributed electronically

ForO 5510.1A

JAN 9 2015

LOCATOR SHEET

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM STANDARD
OPERATING PROCEDURES

Location: _____
(Indicate location(s) of copy(ies) of this Manual)

JAN 9 2015

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 1	BACKGROUND.....	1-1
1.	Basic Policy.....	1-1
2.	Authority.....	1-1
3.	Applicability.....	1-1
4.	Responsibility for Compliance.....	1-1
5.	Items not Addressed.....	1-2
Chapter 2	RESPONSIBILITIES, ADMINISTRATION, AND INSPECTIONS.....	2-1
1.	Basic Policy.....	2-1
2.	Duties and Responsibilities.....	2-1
3.	Security Administration.....	2-6
4.	Security Inspections.....	2-7
5.	Security Managers Meetings.....	2-8
6.	Emergency Action Plans.....	2-8
Figure 2-1	Format for Appointment of Security Manager/Assistant Security Manager....	2-10
Figure 2-2	Format for Appointment of TOP SECRET Control Officer.....	2-11
Figure 2-3	Format for Appointment of North Atlantic Treaty Organization (NATO) Control Officer.....	2-12
Figure 2-4	Format for Appointment of Information Assurance Manager or Cyber Security Officer.....	2-13
Figure 2-5	Format for Appointment of Electronic Key Management System (EKMS)Manager...	2-14
Figure 2-6	Format for Appointment of Special Security Officer (SSO).....	2-15
Chapter 3	CONTINUOUS EVALUATION.....	3-1
1.	Basic Policy.....	3-1
2.	Sabotage, Terrorism, and Compromise...	3-1
3.	Responsibilities.....	3-1
Chapter 4	SECURITY EDUCATION AND TRAINING.....	4-1
1.	Basic Policy.....	4-1
2.	Responsibility.....	4-1

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
3.	Minimum Requirements.....	4-2
4.	Special Briefings.....	4-3
5.	Debriefing.....	4-4
6.	Security Awareness.....	4-4
7.	Security Manager's Required Training..	4-4
Chapter 5	CLASSIFICATION AND MARKING.....	5-1
1.	Basic Policy.....	5-1
2.	Original Classification Authority (OCA).....	5-1
3.	Derivative Classification.....	5-1
4.	Authority to Downgrade, Declassify, or Modify.....	5-1
5.	Marking Derivatively Classified Documents.....	5-2
6.	Notification of Classification Changes.....	5-2
7.	Marking.....	5-2
8.	Marking Classified Information Technology (IT) Media, Systems, and Equipment.....	5-3
Chapter 6	LOSS OR COMPROMISE OF CLASSIFIED MATERIAL.....	6-1
1.	Basic Policy.....	6-1
2.	Administrative Sanctions, Civil Remedies, and Punitive Actions.....	6-1
3.	Definitions.....	6-1
4.	Security Violations.....	6-2
5.	Discovery of Loss, Compromise, or Violation.....	6-2
6.	Loss or Compromise Checklist.....	6-2
7.	Preliminary Inquiry (PI).....	6-3
8.	JAGMAN Investigation.....	6-4
9.	Investigative Assistance.....	6-4
10.	Compromise Through Public Media.....	6-4
11.	Other Security Violations.....	6-4
12.	Unsecured Containers.....	6-5
13.	Unsecured Classified Material.....	6-5
14.	Improper Transmission of Classified Material.....	6-6

JAN 9 2015

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
15.	Information Transmission Systems.....	6-6
16.	Sabotage, Espionage, or Deliberate Compromise.....	6-7
17.	Foreign Contact Reporting Requirements.....	6-7
18.	Foreign Travel.....	6-8
Chapter 7	TRANSMISSION AND TRANSPORT OF CLASSIFIED MATERIAL.....	7-1
1.	Basic Policy.....	7-1
2.	Preparation of Classified Material for Mailing.....	7-1
3.	Shipping Classified Material.....	7-2
4.	Outgoing Mail Log.....	7-2
5.	Return Receipt System.....	7-3
6.	Hand Carrying Classified Material.....	7-3
7.	Facsimile and Other Electronic Data...	7-6
8.	Telephonic Transmissions.....	7-6
Figure 7-1	Format for Authorization to Hand Carry Classified Information.....	7-7
Chapter 8	ACCOUNTABILITY AND CONTROL.....	8-1
1.	Basic Policy.....	8-1
2.	Control Records and Logs.....	8-2
3.	Incoming U.S. TOP SECRET Material.....	8-3
4.	Incoming NATO TOP SECRET Material.....	8-4
5.	Incoming SECRET Material.....	8-4
6.	Inventories Frequency and Scope.....	8-5
7.	Managing Classified Material During Working Hours.....	8-5
8.	End-of-day Security Checks.....	8-5
9.	Classified Meetings.....	8-6
10.	Reproduction of Classified Information.....	8-6
Figure 8-1	Format for Classified Material Inventory.....	8-7

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Figure 8-2	Format for Access and Authorization to Receipt for Classified Material....	8-8
Chapter 9	SECURITY, STORAGE AND DESTRUCTION.....	9-1
1.	Basic Policy.....	9-1
2.	Physical Security Evaluation (PSE).....	9-2
3.	Security Requirements.....	9-3
4.	Storage Requirements.....	9-5
5.	Repairs and Modifications to Security Containers.....	9-9
6.	Methods of Destruction.....	9-9
7.	Destruction Procedures for Classified Material.....	9-10
8.	Destruction Procedures for Classified Hard Drives.....	9-10
9.	Emergency Actions Plan (EAP).....	9-11
10.	Emergency Destruction.....	9-13
Chapter 10	DISSEMINATION, REPRODUCTION AND PHOTOGRAPHY OF CLASSIFIED MATERIAL.....	10-1
1.	Basic Policy.....	10-1
2.	Dissemination.....	10-1
3.	Reproduction Controls.....	10-1
4.	Reproduction Equipment.....	10-2
5.	Photography Controls.....	10-3
6.	Control of Personal Electronic Devices (PED) and Recording Systems.....	10-3
Chapter 11	ACCESS CONTROL AND VISITOR CONTROL.....	11-1
1.	Basic Policy.....	11-1
2.	Visitor Access Control.....	11-1
3.	Visits by Flag/General Officers and Their Civilian Equivalents.....	11-2
4.	Meetings.....	11-2

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 12	PERSONNEL SECURITY INVESTIGATIONS AND SECURITY CLEARANCE ACCESS ELIGIBILITY..	12-1
1.	Basic Policy.....	12-1
2.	Security Indoctrination.....	12-1
3.	Investigative Requirements for Security Clearance Access Eligibility..	12-2
4.	Security Clearance and Investigations..	12-3
5.	Security Clearance Request and Submission.....	12-4
6.	Requests for Additional Information....	12-5
7.	Granting Final Clearance Eligibility...	12-6
8.	Temporary (TEMP/INTERIM) Clearance Access Eligibility.....	12-6
9.	Access Eligibility.....	12-6
10.	Access List.....	12-7
11.	One-Time Access.....	12-7
12.	Access by Reserve Personnel.....	12-7
13.	Suspension of Access.....	12-8
14.	Termination of Access.....	12-9
15.	Investigation Requirements for Access to Sensitive Compartmented Information.....	12-9
16.	Personnel Security Management Network (PSMNET).....	12-9
Chapter 13	INFORMATION TECHNOLOGY (IT) SECURITY PROCEDURES.....	13-1
1.	Basic Policy.....	13-1
2.	IT Positions.....	13-1
3.	Processing Classified Data on IT Equipment.....	13-2
4.	Software Security.....	13-2
5.	System Security.....	13-2
6.	IT Data Security.....	13-3
7.	Destroying Electronic Classified Data..	13-3
8.	Transmission Equipment.....	13-4

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
9.	Spillages.....	13-4
10.	Network Access.....	13-4
11.	Wireless Devices and PED.....	13-5
APPENDIX A	REFERENCES.....	A-1
APPENDIX B	ACRONYMS.....	B-1

JAN 9 2015

Chapter 1

Background

1. Basic Policy. The MARFORRES IPSP is established to ensure that classified information is protected from unauthorized disclosure, and that granting of access to classified information is clearly consistent with the interests of National Security. This Order supplements applicable portions of the references for implementation within MARFORRES Commands and Staff Sections.

2. Authority. COMMARFORRES is responsible for establishing and maintaining an IPSP per the references and directs the MARFORRES Command Security Manager and Deputy Command Security Manager to establish and manage an effective program that complies with all directives issued by higher authority. Commanding Generals (CG), Chiefs of Staff, Directors, Commanding Officers (CO), Inspector-Instructors (I-I), Officers-in-Charge (OIC) of MSC and subordinate units are responsible for establishing and maintaining an IPSP per the references and this Order.

3. Applicability. This Order supplements the provisions of the references and other applicable directives, establishing specific policy and procedures on the handling and security of classified information and material. Information on personnel security provisions published in amplifying or supplemental instructions within this HQ will comply with the policies and procedures of higher HQ directives and this Order.

4. Responsibility for Compliance. COMMARFORRES has overall responsibility for the IPSP for MARFORRES Commands and Staff Sections. This authority is delegated to the MARFORRES Command Security Manager and Deputy Command Security Manager as the responsible officer and subject matter expert. MARFORRES MSC and HQ Staff Sections are responsible for ensuring compliance with this Order.

a. All commands and sections will ensure personnel are properly trained in their responsibilities to safeguard classified information or equipment entrusted to them. They will ensure that only the minimum number of personnel with a need-to-know is authorized clearance and access to classified material.

JAN 9 2015

b. Each individual, military, civilian, or contractor assigned to MARFORRES is responsible for compliance with this Order in all respects. Any procedure or situation, which is a security weakness or could result in an unauthorized disclosure or breach of security, must be reported immediately to the appropriate MSC or Section Security Manager. All security weaknesses, unauthorized disclosures, spillages, or possible breaches of security will be reported to the MARFORRES Command Security Manager or Deputy Command Security Manager.

5. Items not Addressed. This Order supplements existing IPSP directives. It does not fully incorporate all areas of the program. If guidance on a particular matter cannot be found in this Order or identified references, contact the appropriate MSC Security Manager, MARFORRES Command Security Manager or Deputy Command Security Manager.

JAN 9 2015

Chapter 2

Responsibilities, Administration, and Inspections

1. Basic Policy. The COMMARFORRES is directly responsible for an effective IPSP and has delegated the overall coordination and management of command security programs to the MARFORRES Command Security Manager and Deputy Command Security Manager. Responsibilities for various specific areas are further delegated and assigned below. All Commands and Staff Sections are responsible for compliance with and implementation of this Order.

a. All MARFORRES, MSC, and subordinate units shall appoint a Security Manager in writing, refer to Figure 2-1 for sample of appointment letter. Staff Sections will appoint a Security Representative. The Security Manager must be an Officer or civilian employee (General Schedule (GS)-11 or above), with sufficient authority and staff to manage the program for the command. The Security Manager must be a U.S. citizen and have a favorably adjudicated Single Scope Background Investigation (SSBI) for a TOP SECRET clearance completed within the last five years.

b. An Assistant Security Manager appointment is recommended. That person must be a U.S. citizen, and an enlisted service member (E-6) or civilian employee (GS-6) or above. Assistant Security Managers must have an SSBI, TOP SECRET clearance if they are designated to issue interim security clearance eligibilities; otherwise, the investigative and clearance requirements will be determined by the level of access eligibility required by their roles and responsibilities. A minimum SECRET clearance eligibility and access is required.

2. Duties and Responsibilities

a. Command Security Manager. The MARFORRES Command Security Manager serves as the Commander's principal advisor, direct representative, and subject matter expert in matters pertaining to the security of classified information and personnel security management within guidelines established in the references. The Command Security Manager must have an properly adjudicated SSBI background investigation (TOP SECRET Sensitive Compartment Information (TS SCI) Clearance), and must be identified to all MARFORRES personnel by listing name and contact information in organizational charts, telephone

JAN 9 2015

listings, rosters, etc. The Command Security Manager and the Deputy Command Security Manager ensures the implementation, supervision, and coordination of all activities related to information and personnel security rated TOP SECRET and below. All Sensitive Compartment Information (SCI) related issues will be forwarded to the MARFORRES Special Security Officer (SSO). The Command Security Manager will be appointed in writing by the COMMARFORRES. The Command Security Manager and Deputy Command Security Manager will manage the information, personnel, and industrial security program functions and will be guided in the performance of duties by the references and this Order.

b. Duties of the Command Security Manager. The duties of the Security Manager include, but are not limited to:

(1) Manage the implementation and required use of the Joint Personnel Adjudication System (JPAS) and the Electronic Questionnaires Investigation Processing (EQIP) Direct Systems, to initiate, restore, and manage personnel access eligibility, security clearances, and Personnel Security Investigation (PSI) in accordance with the references and this Order.

(2) Ensure security clearance eligibility, access approval, and security clearance and background investigation documentation on Military, Civilian, and Contractor personnel is accurate and current.

(3) Ensure that security measures and procedures regarding visitors who require access to classified information or restricted areas are in compliance with the references and this Order. Access to classified information and spaces is limited to appropriately cleared personnel with a need-to-know, and visitors that have submitted the appropriate visit request in JPAS.

(4) Ensure that NAVMC Functional Area Security Inspections are scheduled and performed on MARFORRES HQ, MSC, and the Marine Corps Support Facility (MARCORSPTFAC) in accordance with the references and this Order.

(5) Perform assist visits and assessments on MARFORRES HQ, MSC, and the MARCORSPTFAC.

(6) Manage the Security Education and Training Program and coordinate and conduct required education and security training as described in the references and this Order.

JAN 9 2015

(7) Maintain personnel security files containing copies of appointment letters, Form 5521, Personal Attestations, In/Out Briefings, Copies of SF85/86, Position Descriptions, and Statements of Work.

(8) Oversee physical security and loss prevention programs and identify property and structures to be protected by ensuring the delegation of function to the appropriate section and coordinating physical security requirements with Federal, State and Local law enforcement and emergency management personnel as appropriate.

(9) Direct the Continuous Evaluation Program with full coordination with medical, Staff Judge Advocate, and HQ Battalion (HQBN), initiating incident reports in JPAS and directing Preliminary Inquiries (PI) and Official Investigations as required.

(10) Ensure that threats to security and other security violations, spillages, and breaches of security are reported, recorded, and when necessary, investigated as described in the references and this Order.

(11) Manage the classification, safeguarding, handling, transmission, and destruction of classified information IAW the references and this Order.

(12) Establish and manage a National Industrial Security Program when the command engages in classified procurement or when cleared contractors operate within command spaces.

c. Deputy Command Security Manager. The Deputy Command Security Manager will be designated in writing by the CO or Command Security Manager. The Deputy Command Security Manager must be a U.S. citizen, and an Officer or civilian employee (GS-11 or above). The Deputy Command Security Manager must have an SSBI and identified to all command personnel by listing name and contact information in organizational charts, telephone listings, rosters, etc. This person's primary duty is to work closely with the Security Manager in all Security Program roles, responsibilities, and functions assigned to the Command Security Manager and described in the references and this Order.

d. Security Assistants. The role of the Security Assistant is to perform security administrative functions and assist the

JAN 9 2015

Security Manager in all actions required to carry out security program requirements under the direction of the Security Manager. The Security Assistant may be assigned, without regard to rate or grade, as long as they are U.S. citizens and have the clearance access required to perform their assigned duties.

e. TOP SECRET Control Officer (TSCO). The TSCO is responsible to the MARFORRES Command Security Manager for the receipt, custody, accountability, and disposition of TOP SECRET material within the MARFORRES HQs as per the references and this Order. All subordinate commands that are currently authorized to hold TOP SECRET material will appoint a TSCO. The security manager may also be appointed as the TSCO. An Officer, enlisted (E-7 or above) or civilian (GS-7 or above) will be assigned duties as the TSCO. The TSCO will have an SSBI completed within the last five years and approved access to TOP SECRET material. The TSCO can appoint at least one TOP SECRET Control Assistant (TSCA). The TSCA will be an enlisted (E-5 or above) or civilian (GS-5 or above) and must have an SSBI with TOP SECRET clearance eligibility and access. MSC subordinate unit appointments will be in writing and approved by the unit OIC. The MARFORRES HQs TSCO will be designated in writing by the MARFORRES Command Security Manager, refer to Figure 2-2 for sample of appointment letter.

f. North Atlantic Treaty Organization (NATO) Control Officer. The NATO Control Officer will be a Staff Non-Commissioned Officer (SNCO) (E-7 or above), civilian (GS-6 or above) and appointed in writing by the MARFORRES Command Security Manager. An assistant can also be appointed in writing. The NATO Control Officer will be guided in the performance of his/her duties by the references and this Order, refer to Figure 2-3 for sample of appointment letter.

g. Information Assurance Manager (IAM) or Cyber Security Officer. Each command involved in processing data in an automated system, including access to local area networks and/or INTRANET or INTERNET, must designate a civilian or military member as an IAM or Cyber Security Officer. An Officer or Senior NCO in charge, in the MARFORRES G-6, will be assigned duties in writing as the IAM for MARFORRES, refer to Figure 2-4 for sample of appointment letter. The IAM implements the MARFORRES information security program and serves as the point of contact for all command information security matters. The IAM will report to the MARFORRES Command Security Manager any incident involving a spillage, breach of security, or issues

that impact information technology (IT), Information Security, or Personnel Security, as required by the references.

h. Electronic Key Management System (EKMS) Manager. By position description a civilian (GS-7 or above), commissioned Officer, or enlisted (E-6 or above) may be assigned as the EKMS Manager, refer to Figure 2-5 for sample of appointment letter. Additionally, the EKMS Manager and Alternate EKMS Manager will be trained and certified as an EKMS Inspectors in order to work as a member of the MARFORRES Inspection Team, responsible for inspecting EKMS accounts of all MARFORRES subordinate units in accordance with the EKMS 3 series. The EKMS 1 series requires that collateral or additional duties assigned to the EKMS Manager must not interfere with the proper management of the Communication Security Management System (CMS) account.

(1) Regardless of service affiliation, both civilian government employees and commissioned officer's appointed must have a minimum of six months government/commissioned service, as applicable which does not include duty under instruction or in training but may include six or more years of prior enlisted service for commissioned officers.

(2) For civilian government employees to be appointed as EKMS Managers or alternates, the position description must specify EKMS Manager duties as a full-time position, prior to appointment as EKMS Manager.

(3) EKMS Managers and alternates must possess a security clearance equal to or higher than the Highest Classification Indicator (HCI) of the account. If the account is validated for/holds keying material intended for use on SCI/SI circuits, both the EKMS Manager and alternates must be SCI eligible and indoctrinated at the time of appointment.

i. Alternate EKMS Manager. Alternate EKMS Managers must at a minimum be an enlisted (E-5 or above), civilian (GS-6/Pay Band 1), or a commissioned officer. For civilian government employees to be appointed as EKMS Managers or alternates, the position description must specify the EKMS Manager duties as a full-time position, prior to appointment as EKMS Manager.

j. Special Security Officer (SSO). The MARFORRES SSO will be an Officer or civilian (GS-9 or above) appointed in writing, refer to Figure 2-6 for sample of appointment letter. Each appointee must be a U.S. citizen, and meet Director, Central

JAN 9 2015

Intelligence Directive (DCID) 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to SCI" (NOTAL) standards. The SSO coordinates his functions with SCI" (NOTAL) standards. The SSO coordinates his functions with the MARFORRES Command Security Manager per Directive C-5105.21 MI (NOTAL) and the references. All MARFORRES Commands will conduct direct liaison with the MARFORRES SSO on all SSO and SCI matters. Although the SSO administers the SCI program independent of the security manager, the MARFORRES Command Security Manager must account for all clearance and access determinations made on members of the command. The MARFORRES SSO will communicate with the MARFORRES Command Security Manager on all matters related to MARFORRES Security Programs. The following duties of the SSO include but are not limited to:

(1) Ensure SCI is properly used, accounted for, controlled, safeguarded, packaged, transmitted, and destroyed in accordance with DoD and Department of the Navy (DoN) directives.

(2) Manage and supervise the SCI Courier Card Program for SCI Facilities (SCIF) under the MARFORRES SCI cognizance.

(3) Maintain the Command SCI billet structure.

(4) Conduct SCI security briefings, education, indoctrinations, and debriefings.

3. Security Administration. Security Managers and/or Assistant Security Managers will prepare and maintain security program turnover files and desktop procedures in a Security Program Binder in order to maintain security program continuity and to better facilitate Command Inspections and the in-briefing of new personnel assuming duties as the Security Manager and Assistant Security Manager. At a minimum, the Security Program Binder will contain a copy of the Functional Area 270 Checklist with the answers to each applicable question along with copies of current appointment letters; a copy of the Command's Security SOP; inspection schedules and copies of prior inspections; a working copy of the Security Servicing Agreement (SSA); copies of all official correspondence relevant to the position; and copies of all custodial documents (inventories, receipts, destruction reports) or a memorandum indicating where they may be found.

a. All Security Managers and Assistant Security Managers will include in their turnover binder information pertaining to

JAN 9 2015

their supervisory role in accomplishing the security policy and procedures set forth in this Order.

b. All Security Managers, Assistant Security Managers, and Security Representatives will maintain personnel security folders for all Command personnel and include completed copies of Form 5521, JPAS Page, Orientation Brief, NATO Brief, Non-Disclosure Agreement (NDA), Personal Attestation Brief (TOP SECRET only), and a copy of the position description for civilian employees.

4. Security Inspections. The MARFORRES Command Security Manager and Deputy Command Security Manager will ensure that Inspector General (IG) Marine Corps Command Inspection Program Functional Area (FA) 270 Security Inspections of MARFORRES Commands and HQ Sections are conducted every 12 to 18 months in order to evaluate and ensure compliance with DoD security program requirements and the following. The Command Security Manager and Deputy Command Security Manager will inspect the IPSP using the NAVMC 5040.6H Functional Area 270 Checklist.

a. Security Inspection Schedule. The MARFORRES Command Security Manager and Deputy Command Security Manager will create and maintain annual Information and Personnel Security Inspection Schedule in accordance with NAVMC DIR 5040.6H, Secretary of the Navy (SECNAV) M-5510.30B, SECNAV M-5510.36, and this Order.

b. Required Security Inspections. MARFORRES Security Managers are required to perform regular Security Inspections on their assigned subordinate commands every 12 to 18 months. Security Inspections and Unannounced Security Inspections (USI) will be conducted throughout MARFORRES using the FA 270 checklist to ensure that the functional areas of the IPSP are managed and maintained in accordance with the FA 270 checklist and the references.

c. Security Inspectors. Security Inspections will be conducted by trained and certified security inspectors who have completed the USMC Security Managers Course, hold a minimum of SECRET security clearance eligibility, and maintain a current Security Manager Appointment letter.

d. Security Inspection Procedures. The following procedures will govern the conduct of regular Scheduled Security Inspections and USI:

JAN 9 2015

(1) Members of the inspecting team will present their credentials and their U.S. Armed Forces Identification Common Access Card (CAC).

(2) The Site Security Manager or his security assistant will accompany the inspectors.

(3) During the inspection, command personnel will open locked working spaces at the Security Inspector's request. If keys or combinations to these spaces are not available, command personnel will recall the appropriate personnel to open the space, at the discretion of the senior inspector.

(4) If classified material is found unsecured by the inspectors, the individual responsible for the material will be notified by the command representative to report and secure the material. If appropriate, an inventory will be immediately initiated.

(5) If the Security Inspections are conducted after hours, command duty personnel will log in the identities of the inspectors, the time the inspection began and ended, and the results of the inspection.

e. Command Assessment Report. Upon completion of the Security Inspection, the senior inspector will draft a Command Assessment Report within 30 days of the inspection. After review, the Command Security Manager or Deputy Command Security Manager will transmit a copy of the report to the MARFORRES Chief-of-Staff, MARFORRES IG, and the cognizant Site Commander or Staff Section OIC.

5. Security Managers Meetings. The MARFORRES Command Security Manager or the Deputy Command Security Manager will periodically hold a Security Management Meeting (Security Forum) to provide and receive input on new information on all MARFORRES Security Programs, and changes in security policies and procedures, and call attention to issues within specific MARFORRES security programs.

6. Emergency Action Plans (EAP). The EAP is designed for the coordination and protection of personnel, classified material, and assets in case of CBRN or fire/smoke emergency, natural disaster, civil disturbance, or enemy action. CO shall develop an emergency plan for the protection of classified information in case of a natural disaster or civil disturbance.

JAN 9 2015

This plan may be prepared in conjunction with the command's disaster preparedness plan and will include plans for emergency protection and destruction of classified material. The MARFORRES Command Security Manager or the Deputy Command Security Manager will ensure that the CO, MARCORSPTEAC, Facilities Chief-of-Staff, Anti-Terrorism Force Protection (ATFP) Program Manager, EKMS Manager, Emergency Management Officer, and the SSO work together to develop a fully coordinated EAP for the protection of MARFORRES Commands and the MARCORSPTEAC. EAP will be published and briefed to each section and subordinate unit, and tested and reviewed on a regular basis.

JAN 9 2015

(Unit Letterhead)

5510

(SECTION)

Date

From: Commander, Marine Forces Reserve or Unit/Site Commander
To: (Rank, Name, EDIPI of Appointee)

Subj: APPOINTMENT OF MARFORRES (UNIT) SECURITY MANAGER or
ASSISTANT SECURITY MANAGER

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) ForO 5510.1A
(d) (Unit Security SOP)

1. You are hereby appointed as the (COMMAND) Security Manager or (Assistant Security Manager) vice (Rank, Name, EDIPI of previous appointee), who stands relieved.

2. You will familiarize yourself with the duties, policies, and procedures set forth in the references.

3. This assignment will remain in effect until you are formally relieved or transferred.

Signature

Copy to:
Adjutant
SMO

Figure 2-1. --Format for Appointment of Security
Manager/Assistant Security Manager

JAN 9 2015

(Unit Letterhead)

5510
(SECTION)
Date

From: Commander, Marine Forces Reserve or Unit/Site Commander
To: (Rank, Name, EDIPI of Appointee)

Subj: APPOINTMENT AS TOP SECRET CONTROL OFFICER

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) OPNAVINST C5510.101
(d) ForO 5510.1A

1. You are hereby appointed as the TOP SECRET Control Officer.
2. You will familiarize yourself with the duties, policies, and procedures set forth in the references.
3. This assignment will remain in effect until you are formally relieved or transferred.

Signature

Copy to:
MARFORRES Command Security Manager
Unit Security Manager

Figure 2-2. --Format for Appointment of TOP SECRET
Control Officer

JAN 9 2015

(Unit Letterhead)

5510
(SECTION)
Date

From: Commander, Marine Forces Reserve or Unit/Site Commander
To: (Rank, Name, EDIPI of Appointee)

Subj: APPOINTMENT AS NORTH ATLANTIC TREATY ORGANIZATION (NATO)
CONTROL OFFICER

Ref: (a) SECNAV M-5510.30
(b) SECNAV M-5510.36
(c) OPNAVINST C5510.101
(d) ForO 5510.1A

1. You are hereby appointed as the NATO Control Officer.
2. You will familiarize yourself with the duties, policies, and procedures set forth in the references.
3. This assignment will remain in effect until you are formally relieved or transferred.

Signature

Copy to:
MARFORRES Command Security Manager
Unit Security Manager

Figure 2-3. --Format for Appointment of North Atlantic
Treaty Organization (NATO) Control Officer

JAN 9 2015

(Unit Letterhead)

5510
(SECTION)
Date

From: Assistant Chief of Staff, G-6 (or Unit Commander)

To: (Rank, Name, EDIPI of Appointee)

Subj: APPOINTMENT AS INFORMATION ASSURANCE MANAGER (IAM) OR
CYBER SECURITY OFFICER

Ref: (a) DoD Dir 8500.1

(b) DISA Instruction 630-230-19

1. You are hereby appointed as the Information Assurance
Manager (IAM).

2. You will familiarize yourself with the duties, policies, and
procedures set forth in the references.

3. This assignment will remain in effect until you are formally
relieved or transferred.

Signature

Copy to:

MARFORRES Command Security Manager

Figure 2-4. --Format for Appointment of Information
Assurance Manager or Cyber Security Officer

ForO 5510.1A
JAN 9 2015

(Unit Letterhead)

5510
(SECTION)
Date

From: Commander, Marine Forces Reserve or Unit/Site Commander
To: (Rank, Name, EDIPI of Appointee)

Subj: ASSIGNMENT OF ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS)
MANAGER

Ref: (a) EKMS 1 (series)

1. In accordance with the reference, you are hereby appointed as (EKMS Manager, Alternate EKMS Manager, Local Element (Issuing), STE User Representative, LMD UNIX System Administrator, or EKMS Clerk/Accountant) for this command.

2. EKMS account number: _____.

3. EKMS COI (V-4C-0013) completed on (YYMMDD) at (name/location of EKMS COI), as applicable. If a quota has been obtained but training not yet completed, annotate the class convening date and prepare an updated appointment letter or affix the completion certificate to the appointment letter when training is completed.

4. Security clearance: (TOP SECRET/SECRET, etc., as applicable).

Signature

Copy to:
MARFORRES Command Security Manager

Figure 2-5. --Format for Appointment of EKMS Manager

JAN 9 2015

(Unit Letterhead)

5510
(SECTION)
Date

From: Commander, Marine Forces Reserve or Unit/Site Commander
To: (Rank, Name, EDIPI of Appointee)

Subj: APPOINTMENT AS SPECIAL SECURITY OFFICER (SSO)

Ref: (a) DoD S-5105.21-M-1 Administrative Security manual
(b) DoD C-5105.21-M-1 Navy Department Supplement
(c) DoD TS-5105.21-M-2 SCI Security Manual

1. You are hereby appointed as the Special Security Officer (SSO).
2. You will familiarize yourself with the duties, policies, and procedures set forth in the references.
3. This assignment will remain in effect until you are formally relieved or transferred.

Signature

Figure 2-6. --Format for Special Security Officer

JAN 9 2015

Chapter 3

Continuous Evaluation

1. Basic Policy. COMMARFORRES has overall responsibility for the continuous evaluation, investigation and security management of all MARFORRES personnel and functions. This authority is delegated to the MARFORRES Command Security Manager as the responsible officer and subject matter expert. All military and civilian personnel, whether they have access to classified information or not, will report to their security managers, COs, or to the nearest command any activities described in this chapter involving themselves, their dependents, co-workers, or others.

2. Sabotage, Terrorism, and Compromise. Personnel that become aware of any plans or acts of sabotage, terrorism, espionage, deliberate compromise, or other subversive activities will report all available information concerning such activities immediately to the security manager, CO at their command, or a senior supervisor at the most readily available command. The command receiving the report shall promptly notify the servicing Naval Criminal Investigative Service (NCIS) office.

3. Responsibilities. COs are responsible for establishing and administering a program for continuous evaluation. Supervisors and managers play a critical role in assuring the success of the continuous evaluation program. Keys to an active continuous evaluation program are security education and positive reinforcement of reporting requirements in the form of management support confidentiality and employee assistance referrals. The goal is early detection of an individual's problems therefore continuous evaluation reporting is vital as the information protects the classified assets and the people that hold the clearance access eligibility. Continuous evaluation requirements are outlined in SECNAV M-5510.30, chapter 10.

a. Reporting Requirements. The continuous evaluation program will rely on all personnel within the command to report questionable or unfavorable information that may be relevant to a security clearance determination. All personnel are required to report any suspicious behavior, violence, or circumstances that are out of the ordinary to their supervisor or appropriate

JAN 9 2015

security manager. All personnel who possess a security clearance are to report to their CO, and/or security manager, any behavior or situation based on the following:

(1) Report any instance where an individual or group makes contact and asks to gain illegal or unauthorized access to classified or otherwise sensitive information.

(2) Report to the command any concerns that you, or someone you know, may be the target of exploitation.

(3) Report any information with potential to impact security clearance eligibility or access, or impact the safety or security of command personnel.

(4) Report suspicious or potentially violent behavior.

(5) Report any involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the U.S. by unconstitutional means.

(6) Report any foreign influence concerns or close personal association with foreign nationals or nations.

(7) Report foreign citizenship (dual citizenship) or foreign monetary interests.

(8) Report any sexual behavior that is criminal, or reflects a lack of judgment or discretion.

(9) Report any conduct involving questionable judgment, untrustworthiness, unreliability, unwillingness to comply with rules and regulations, or unwillingness to cooperate with security clearance processing.

(10) Report any unexplained affluence or excessive indebtedness.

(11) Report any alcohol abuse or drug involvement.

(12) Report any apparent mental, emotional, or personality disorder.

(13) Report any incident or noncompliance with security requirements, that would affect clearance or access eligibility.

JAN 9 2015

(14) Report any suicide or attempted suicide.

(15) Report any personnel that are in an Unauthorized Absence (UA) status.

b. If any MARFORRES personnel attempts to commit suicide and is referred for treatment, the MARFORRES Command Security Manager or Deputy Command Security Manager will be notified. The Security Manager will initiate an incident report in JPAS and ensure that a debriefing/counseling with the individual is conducted. If the individual is a security representative or a key custodian and had access to classified material, all related combinations and access codes will be changed and a classified material inventory will be conducted immediately.

c. If the individual in a UA status had access to security containers or a classified area, all related combinations and access codes will be changed and a classified material inventory will be conducted immediately. If a PI is conducted and reveals indications that national security may be adversely affected, the servicing NCIS office will be immediately notified by the Command Security Manager or Deputy Command Security Manager. Suspension of access is required when a military member with a security clearance is declared a deserter or is absent without leave for a period exceeding 30 days.

JAN 9 2015

Chapter 4

Security Education and Training

1. Basic Policy. COMMARFORRES has overall responsibility for the Security Administration function and the Education and Training Program for MARFORRES Commands and Sections. This authority is delegated to the MARFORRES Command Security Manager or Deputy Command Security Manager as the responsible officer and subject matter expert. The goal of the MARFORRES Security Education and Training Program is to ensure that all personnel understand security requirements and procedures; the critical need to understand and protect personnel and classified information, assets, and spaces; and to develop fundamental habits of security so that proper discretion and judgment will be automatically exercised in the discharge of duties involving security programs as a whole.

2. Responsibility. The MARFORRES Command Security Manager is responsible for overall policy guidance, establishing Security Education and Training requirements, and coordinating support. Security Education and Training guidelines for courses of instruction and new information are available on the MARFORRES Share Portal.

a. Command Security Manager. The Command Security Manager or the Deputy Command Security Manager will ensure all MARFORRES personnel receive the required annual Security Education training. The HQBN Training Officer will assist the Security Management Office in coordinating training spaces and making arrangements for training and will ensure that appropriate training records documenting Security Education and Training are maintained and entered into the Marine Corps Total Force System (MCTFS) per current training directives.

b. Site Security Managers and Security Representatives. Security Managers and Security Representatives are responsible for ensuring that their assigned personnel complete annual security education training and print completion certificates as required by the on-line or onsite training course of instruction. All MARFORRES Commands and Sections that handle or process classified material will ensure that supplemental on-the-job-training (OJT) is also made available to their personnel.

JAN 9 2015

3. Minimum Requirements

a. Indoctrination Brief. All personnel must have a basic understanding of what classified information is and how/why classified information is safeguarded. Military members will receive a security indoctrination brief upon check-in. The Security Manager will ensure that all military, civilian, and contractor personnel reporting to a MARFORRES Command are briefed as to the requirements of maintaining a security clearance and the importance of Security Awareness, continuous evaluation, and Security Programs as a whole. The indoctrination process is a critical function of the check-in process and all personnel will have a personnel security folder created that will include a copy of; completed Form 5521, signed NDA (SF312), signed Orientation Brief, their JPAS page, their Position Description (PD) or contract. All personnel checking-in will be updated in JPAS.

b. Orientation Brief. Each person who requires access to classified information will receive an orientation brief prior to being granted access to classified information. The brief will be tailored to address the specific procedures and requirements within the command restricted areas and open storage SECRET spaces.

c. On-The-Job-Training (OJT). MARFORRES OICs and/or supervisors will ensure that subordinates understand the general security requirements and those security responsibilities specific to their individual duties. The primary responsibility of supervising OJT rests with the OICs and/or supervisors.

d. Refresher Training. The MARFORRES Command Security Manager will direct regular security refresher briefings for all MARFORRES personnel per the references. Unit Security Managers are directed to schedule and manage security training at the subordinate unit levels. Refresher training will be designed to reinforce security awareness and reporting of any issue related to security of personnel and property, and to motivate fulltime security discipline across the Force. Personnel will be advised of the requirement to report foreign travel. Changes in security policies and procedures, security alerts, positive and negative trends noted in any security program, and special security considerations, such as the processing of classified information on computers, are examples of other appropriate subjects for refresher training.

JAN 9 2015

e. Counterespionage Briefing. Personnel with access to classified material will receive a counterespionage briefing annually. The Security Manager can arrange with the local NCIS offices to give this brief. Subordinate units that are not located near a NCIS office can request assistance from their higher headquarters.

f. ATFP/Operational Security (OPSEC) Brief. At least once annually all Military, Civilian, and Contractor personnel are required to receive OPSEC Training. All personnel are required to receive this brief prior to traveling overseas. Only a certified Anti-Terrorism Training Officer (ATTO) is authorized to give this brief. Contact the Security Manager or the Mission Assurance Office for the name of the Anti-Terrorism Officer (ATO) within your MSC.

4. Special Briefings

a. Foreign Travel Brief. A foreign travel brief is required when traveling outside the continental United States (OCONUS). Contact the Mission Assurance Office for foreign travel briefing requirements. Individuals with SCI indoctrinated access will be referred to the MARFORRES SSO for a foreign travel briefing. Upon return to the United States personnel will notify the Mission Assurance Office or the MARFORRES SSO to schedule a debriefing.

b. SCI Brief. The SSO or Assistant SSO will indoctrinate and approve access to the SCI Program and the SCIF.

c. NATO. All personnel who require access to NATO information are required to complete and sign a NATO security procedures briefing. The NATO briefing is performed by the Security Manager or the NATO Officer.

d. Classified Material Courier Brief. Prior to authorizing a traveler to hand carry classified material, the Security Manager will brief the individual on the proper responsibilities and procedures to be followed per the references. A courier letter or courier card will be issued and signed by the Security Manager. Classified material cannot be transported out of the restricted area without a signed courier letter or courier card.

JAN 9 2015

5. Debriefing. Personnel who have had access to classified information must be debriefed and appropriate security termination forms will be completed by the Security Manager under the following circumstances:

- a. Upon check-out and prior to termination of active military service or civilian employment;
- b. When security clearance eligibility is revoked for cause or administratively withdrawn;
- c. When the individual has inadvertently gained access to classified information that he/she was not eligible to receive.

6. Security Awareness. All Security Managers will establish procedures for the dissemination of current security information via signs, poster, bulletins, memorandums, electronic mail, or other means. Security Managers will ensure widest dissemination of all security related information.

7. Security Manager's Required Training. All personnel designated as a Security Manager or Assistant Security Manager must complete the U.S. Marine Corps Security Managers Course within 90 days of their appointment. Information regarding the Marine Corps Security Managers Course can be found on the MARFORRES Security SharePoint Portal. Requests to attend the Marine Corps Security Managers Course will be routed through the appropriate chain of command to the MARFORRES Security Management Office. A record of completion will be maintained with the letter of appointment in the Command's Security Program Binder. A copy of the letter will be forwarded to the MARFORRES Command Security Manager.

JAN 9 2015

Chapter 5

Classification and Marking

1. Basic Policy. COMMARFORRES has overall responsibility for the classification and marking of MARFORRES classified material. This authority is delegated to the MARFORRES Command Security Manager as the responsible officer and subject matter expert.
2. Original Classification Authority (OCA). The authority to be an OCA and originally classify information as TOP SECRET, SECRET, or Confidential rests with the SECNAV and delegated to HQ Marine Corps (HQMC) as the designated OCA for MARFORRES. Original classification is the initial decision that an item of information could be expected to cause damage to the national security if subjected to unauthorized disclosure. This decision shall be made only by OCA who have been specifically delegated the authority to do so, have received training in the exercise of this authority, and have program responsibility or cognizance over the information.
3. Derivative Classification. Derivative classification is the incorporating, paraphrasing, restating, or generating, in new form, information that is already classified and the marking of newly developed information consistent with the classification markings that apply to the classified source. This includes the classification of information based on classification guidance or source documents.
4. Authority to Downgrade, Declassify, or Modify. The only officials authorized to downgrade, declassify, or modify an original classification determination with a resulting change in the classification guidance for classified DoN information are:
 - a. The SECNAV with respect to all information over which the DoN exercises final classification authority.
 - b. The DoN OCA who authorized the original classification or that OCA's current successor.
 - c. The next superior in the chain-of-command provided that official is an OCA.
 - d. The authority to downgrade, declassify, or modify is not to be confused with the responsibility of an authorized holder

JAN 9 2015

of the classified information to downgrade, declassify, or modify it as directed by classification guidance or the cognizant OCA.

5. Marking Derivatively Classified Documents. Mark the face of a document containing only derivatively classified information with a "Derived from" line. If all of the information was derivatively classified using a single Security Classification Guide (SCG) or source document, identify the SCG or source document on the "Derived from" line. Include the date of the source document or SCG (unless the identification of either the source or the SCG implicitly includes the date) per reference (b) exhibit 6A-8.

6. Notification of Classification Changes. OCA are responsible for notifying holders of any classification changes involving their information. Original addressees and holders shall be notified of an unscheduled classification change such as classification duration, or a change in classification level.

7. Marking. Marking of classified material is a critical function in information security management. The MARFORRES Command Security Manager is charged with ensuring that classified material is properly marked and managed. All classified documents will be marked by (stamp, print, or permanently affix with a sticker or tape) on the face and back cover, top and bottom center, of all classified documents to show the highest overall classification level of the information they contain. This marking shall be conspicuous enough to show it is classified. This requirement also applies to emails on classified Information Technology (IT) systems (e.g., SIPRNET). All classified information shall be clearly marked with the date and office of origin, the appropriate classification level and all required "associated markings" include those markings that identify the source of classification (or for original decisions, the authority and reason for classification); downgrading and declassification instructions; and warning notices, intelligence control markings and other miscellaneous markings as per SECNAV M5510.36 paragraph 6-7.

a. Marking IT. Marking is required on IT systems and electronic media, including removable components that contain classified information as per reference (b), paragraph 6. IT systems include any equipment or interconnected system that is used in the storage, management, movement, or reception of data or information. Electronic media includes Universal Serial Bus

JAN 9 2015

drives, flash drives, compact disks, scanners, videotapes, disks, recordings, etc. IT systems that process classified data in forms other than traditional documents, such as weapon, navigation, and communication systems also require appropriate marking.

b. Classification Level and Associated Markings.

Classification level and associated markings shall not be applied to any classified article or portion of an article that has appeared in the public domain. Classified documents provided to foreign governments, their embassies, missions, or similar official offices within the U.S., shall be marked as described in reference (b), chapter 6. Classified documents shall not be marked if the markings themselves would reveal a confidential source or relationship, or a confidential human intelligence source not otherwise evident in the document.

8. Marking Classified Information Technology (IT) Media, Systems, and Equipment. Classified removable IT storage media will be marked with the highest overall classification level using the appropriate label (SFs 706, 707, 708, 709, 710, and 712 (for SCI IT media)) and include the abbreviated form of all applicable warning notices and intelligence control markings per reference (b), chapter 6. Removable IT storage media is any device in which classified data is stored and is removable from a system by the user or operator (i.e., optical disks, magnetic diskettes, removable hard drives, thumb drives, tape cassettes, etc.).

a. Any classified IT media, systems, and equipment shall be marked to indicate the highest classification level of the information processed by the IT system and the network to which it is connected. This is especially important with systems that have the capability to switch from a classified network connection to an unclassified network or system. The appropriate label (SFs 706, 707, 708, 709, 710, and 712 (for SCI IT media)) shall be placed on IT systems and components with memory such as workstations, external hard drives, printers, copiers, portable electronic devices, servers, and back-up devices.

b. IAMS and Cyber Security Managers shall ensure that IT systems provide a classification designation of data stored in internal memory or maintained on fixed storage media.

JAN 9 2015

Chapter 6

Loss or Compromise of Classified Material

1. Basic Policy. The loss or compromise of classified information presents a threat to National Security. The seriousness of that threat must be determined and measures taken to negate or minimize the adverse effects of the compromise. COMMARFORRES has overall responsibility for the ensuring the security of classified material and to ensure security incidents or violations, involving MARFORRES Commands and Staff Sections, are appropriately managed. This authority is delegated to the MARFORRES Command Security Manager or Deputy Command Security Manager as the responsible officer and subject matter expert. All security incidents or violations will be expeditiously reported, vigorously investigated, and corrective action taken to prevent a recurrence of the violation.

2. Administrative Sanctions, Civil Remedies, and Punitive Actions

a. Civilian and contractor employees are subject to administrative sanctions, civil remedies, and criminal penalties if they knowingly, willfully, or negligently disclose classified information to an unauthorized person or violate the provisions of the references or this Order.

b. Military personnel are subject to punitive action, either in federal courts or under the Uniform Code of Military Justice, as well as administrative sanctions, if they disclose classified information to any unauthorized person, or violate the provision this Order, the references, or any new security directives.

3. Definitions

a. Loss of classified information. Loss of classified information occurs when it cannot be physically accounted for or located.

b. Compromise. A compromise is the unauthorized disclosure of classified information to a person(s) who does not have valid clearance access eligibility and the need-to-know.

c. Possible Compromise. A possible compromise or spillage occurs when classified information is not properly controlled.

JAN 9 2015

d. Breach. A breach is when a secure area is intentionally entered by person(s) that do not have valid clearance access eligibility and the need-to-know and classified material is compromised or removed.

4. Security Violations. A security violation, spillage, or security incident will be vigorously investigated with the intent of identifying the security weakness or failure causing the violation; the person(s) involved, and if any classified material or spaces have been compromised. All findings must be documented and shall include recommendations for corrective action to ensure the violation will not occur again.

5. Discovery of Loss, Compromise or Violation. Any individual who becomes aware of the loss, possible compromise, or actual compromise of classified information or material will immediately notify the MARFORRES Command Security Manager or Deputy Command Security Manager. At a minimum, the Command will conduct a Preliminary Inquiry (PI) in every case.

a. The MARFORRES Command Security Manager or Deputy Command Security Manager will be notified in all situations where any loss, compromise, possible compromise, or breach of security has occurred.

b. The MSC Security Manager will notify the MARFORRES Command Security Manager or Deputy Command Security Manager who will then notify the MARFORRES G-6 in any situation that involves communications, messages, or computers regarding spillage, loss, compromise, possible compromise, or a security breach.

c. Any spillage, or incident involving classified material or compromise on a computer system will be reported to the MARFORRES G-6 Cyber Security Officer and the MARFORRES Command Security Manager or Deputy Command Security Manager within 24 hours.

6. Loss or Compromise Checklist. The following is a checklist of immediate actions that must take place once a loss, compromise, or possible compromise of classified material has been discovered:

_____ Has the material/safe/equipment and all unauthorized copies been secured?

JAN 9 2015

- _____ Has the chain of command been notified? If so, who/when: _____
- _____ Has the MARFORRES Command Security Manager or Deputy Command Security Manager been notified?
- _____ Has NCIS been notified? If so, who/when: _____
- _____ Will NCIS be conducting an investigation?
- _____ Was it necessary to contact the MARFORRES G-6 due to a spillage or computer asset compromise?
- _____ Has the appropriate MSC Security Manager been notified? If so, who/when: _____
What guidance was provided? _____
- _____ If the violation/discrepancy involved an open security container or missing material was an inventory conducted? If so, who/when: _____
- _____ Has someone been appointed to conduct the preliminary inquiry (PI)? If so, who: _____
If no, were the appropriate parties notified? _____
- _____ Was the PI forwarded to the MARFORRES Command Security Manager?
- _____ Were the corrective measures noted in the PI?
- _____ Did the PI indicate a Judge Advocate General Manual (JAGMAN) investigation should be conducted?
- _____ Were the corrective measures noted in the investigation implemented?

7. Preliminary Inquiry (PI). If classified information has been lost, compromised, or subjected to compromise, a PI will be conducted. The Security Manager is responsible for initiating the PI and ensuring an appropriate investigation is completed. The PI will be completed within 72 hours unless an extension has been granted by the Security Manager.

JAN 9 2015

a. The CO, or designated Security Manager, will appoint an investigating Officer to conduct the PI.

b. Every effort will be made to keep the PI unclassified. The fact that a compromise has occurred is not necessarily classified.

c. Specific guidelines for conducting a PI are contained in reference (b), Chapter 12.

d. If the inquiry determines that compromise was possible and that the probability of damage to national security cannot be discounted, significant activity weakness is revealed, or punitive action is appropriate, a JAG Manual Investigation will be initiated.

8. JAGMAN Investigation. The purpose of the JAGMAN investigation is to answer, in detail, who, what, where, when, why, and how, questions concerning the security violation. Guidance for conducting a JAGMAN investigation is contained in reference (b), Chapter 12. The investigating officer will consult with the Staff Judge Advocate before initiating a JAGMAN Investigation.

9. Investigative Assistance. The MARFORRES IG, Command Security Manager or Deputy Command Security Manager, NCIS, or another DoD or federal agency may be required to assist the Investigation Officer in an investigation. Investigative assistance will be coordinated through the Command Security Manager.

10. Compromise Through Public Media. It is a security violation to replicate classified information on unclassified networks. Notify the MARFORRES Command Security Manager or Deputy Command Security Manager in any case where classified information may have been compromised as a result of disclosure in the public media, (i.e., newspapers, books, radio, or television broadcasts). Provide as many details as possible, such as the name of the reporter, newspaper, television show, dates, and station. The MARFORRES Command Security Manager or Deputy Command Security Manager are responsible for notifying the MARFORRES PAO and forwarding this information to CNO (NO9N2) and NCIS as per the references.

11. Other Security Violations. Violations of security regulations, which do not result in a compromise or subsection

JAN 9 2015

to compromise, may be acted upon by the MSC chain of command without reporting to higher authority. However, if the circumstances of the security violation impact the COMMARFORRES and/or constitute a national security case, the MARFORRES Command Security Manager or Deputy Command Security Manager will be notified.

12. Unsecured Containers. A major security violation occurs when a container in which classified material is stored is found unsecured in the absence of cleared personnel, with proper access eligibility. Unless the room has been specifically approved for open storage this is a reportable security violation. If such an incident occurs during working hours, the Security Manager will be immediately notified.

a. If the incident occurs after normal working hours the Duty Officer and the security manager will be notified immediately and the following steps will be taken:

(1) The custodian(s) whose name is listed in the locking drawer of the security container, or on the inside of the storage area door, will be notified immediately.

(2) The Duty Officer will notify the Security Manager. The Security Manager will provide the Duty Officer additional guidance, as required.

(3) The person discovering the open container will remain in the vicinity of the open security container or storage area door until the custodian arrives.

(4) The custodian will conduct a complete inventory of the security container or storage area. A written report will be made to the Security Manager detailing any discrepancies or missing documents.

(5) The person discovering the open container will prepare a written statement describing the circumstances leading to the discovery. The statement will remain on file with the Security Manager, and a copy will be forwarded to the MARFORRES Command Security Manager.

13. Unsecured Classified Material. If an item of classified material is found unsecured (e.g., unattended on a desk, on the deck, in the trash), the finder will immediately secure the

JAN 9 2015

material from further disclosure and hand carry it to Security Manager or, if after working hours, to the Duty Officer. The Duty Officer will ensure that the material is properly safeguarded until the Security Manager is notified and responds to take custody of the material. A written report detailing the circumstances of the discovery and disposition of the material will be made to the MARFORRES Command Security Manager or Deputy Command Security Manager.

14. Improper Transmission of Classified Material. When an individual discovers that classified material or equipment has been improperly transmitted/shipped, or damaged in shipment, the individual will notify the Security Manager immediately. The Security Manager will initiate a PI into the incident, and continuous correspondence will be maintained with the MARFORRES Command Security Manager as per chapter 12 of reference (b), and this Order.

15. Information Transmission Systems. Report any possible spillage, loss, physical compromise, or suspected compromise of any information transmission systems related equipment to the Command Security Manager or Deputy Command Security Manager, Cyber Security Officer, or Information Assurance Office. If a spillage, loss, physical compromise, or suspected compromise has occurred, a PI will be conducted per the references and this Order. If an email is received or a site is identified that may have classified information, e.g. a document with classified markings, operational information or dates, locations, or numbers of personnel or equipment notify the Cyber Security or Information Assurance Office. The Cyber Security or Information Assurance Office will confirm if a spillage occurred, and will give instructions for follow on actions that must take place. For a spillage, physical compromise, or suspected compromise follow the guidance below.

a. Do not download, print, or forward the information to anyone.

b. Report the email or site with the possible classified information spillage to the local Cyber Security or Information Assurance Office.

c. For more information see the C4 policy on incident reporting at <https://c4.hqi.usmc.mil/>.

JAN 9 2015

16. Sabotage, Espionage, or Deliberate Compromise. Anyone who see or hears of a possible act of terrorism, sabotage, espionage, or deliberate compromise of security will immediately contact their Security Manager and supervisor. The MARFORRES Command Security Manager or Deputy Command Security Manager will be notified immediately on any issue involving the security of classified material and the protection of personnel and assets on any MARFORRES Command, the MARCORSPTEFAC, or related to MARFORRES Commands in general.

a. The Security Manager will notify the MARFORRES Counterintelligence Officer and the servicing NCIS office immediately of any requests (elicitations), for classified information or unclassified technical data with military or space applications that may constitute attempted espionage. Examples of unclassified requests (elicitations) include; information on personnel, names, operations, security, duties, technical orders, technical manuals, regulations, military phone books, personnel rosters, unit manning tables, unit strength, mission, combat readiness, and development or effectiveness of weapon systems.

b. The MARFORRES Command Security Manager or Deputy Command Security Manager will be contacted by the most expeditious means with details concerning the incident. All available information (who, what, when, where, why, and how) will be provided.

17. Foreign Contact Reporting Requirements. Individuals are responsible for prompt reporting of any attempts by an individual, regardless of nationality, to elicit or aggressively inquire into any classified or otherwise sensitive aspects of their work. All personnel possessing a DoD security clearance eligibility must:

a. Report all contacts with individuals of any nationality who request unauthorized or illegal access to classified or otherwise sensitive information.

b. Report any contact with an individual (regardless of nationality) if it is suspected being targeted for exploitation, or the individual takes in-depth interest in duties, workplace, or the personnel work with and their specific duties.

JAN 9 2015

c. All suspicious contacts are to be immediately reported to the MARFORRES Command Security Manager, Deputy Command Security Manager, and the Counterintelligence Officer.

18. Foreign Travel. Military and Civilian personnel are required to notify their supervisor prior to foreign travel. MARFORRES personnel are required to notify the MARFORRES G-3/5 Mission Assurance Program Manager to schedule a foreign travel briefing. MARFORNORTH personnel will contact the MARFORNORTH physical security officer for notification and approval.

JAN 9 2015

Chapter 7

Transmission and Transport of Classified Material

1. Basic Policy. COMMARFORRES has overall responsibility for the ensuring the security of classified material and to direct the proper transmission and transport of classified material. This authority is delegated to the MARFORRES Command Security Manager or Deputy Command Security Manager as the responsible officer and subject matter expert. Reference (b), chapter 9 sets forth the policies and procedures for the hand carrying, transmission, and transport of classified material by any Marine Corps or Navy personnel.

2. Preparation of Classified Material for Mailing. The Command Security Manager will establish procedures for training and equipping security personnel to properly prepare and ship classified material. MARFORRES HQs Commands and Sections will package and ship classified material in the Security Management Office. Classified material shipped to the MARFORRES HQs or a MSC HQs will be received by the Security Management Office and logged. Outside commands will ship the classified material to; MARFORRES, Attn: Security Management Office, Suite. 4E5500, 2000 Opelousas Ave, New Orleans, LA, 70114. EKMS material will be prepared and shipped by the MARFORRES EKMS Manager and SCI material will be prepared and shipped by the MARFORRES SSO.

a. Wrapping prior to shipment. Personnel preparing the package for shipment will mark, wrap, label, and address each package in the following manner.

(1) Classified material transported outside a facility must be double-wrapped, (enclosed in opaque inner and outer containers).

(2) The inner envelope shall be sealed and marked with the receiver's and the sender's classified mailing addresses, the highest classification of the contents and any appropriate caveats.

(3) The outer envelope shall be marked with the receiver's and the sender's classified mailing addresses.

(4) No markings or notations on outer envelope shall be made indicating that the contents are classified.

JAN 9 2015

(5) Prepare classified information for shipment by packaging and sealing it with tape which will retain the impression of any postal stamp, in ways that minimize risk of accidental exposure or undetected deliberate compromise.

(6) Classified information shall be packaged so that classified text is not in direct contact with the inner envelope or container.

3. Shipping Classified Material. Classified material will be shipped via registered USPS or an Express ground or air shipping company, and marked, wrapped, labeled, and addressed in each package in accordance with the references. Overnight carriers are authorized to ship SECRET and CONFIDENTIAL material when the material has been prepared in accordance with this chapter and reference (b), Chapter 9.

a. TOP SECRET material will only be transmitted as outlined in paragraph 9-2 of reference (b).

b. SECRET and CONFIDENTIAL will only be transmitted as outlined in this chapter and reference (b).

c. To ship SECRET material OCONUS use the Defense Courier Service only when a DoD or Government courier cannot be utilized.

d. Under no circumstances will the "waiver of signature and indemnity" block of the Express Mail Label be executed.

e. TOP SECRET material shipped to the MARFORRES HQs will be received by the MARFORRES TSCO. Classified material rated and SECRET material and or below will be received by the Command Security Manager or the Deputy Command Security Manager, and hand carried to the appropriate Command or Staff Section.

4. Outgoing Mail Log. The outgoing registered mail log or automated file shall contain at a minimum the following information:

a. Registered Mail Number

b. Serial Number

c. Classification

JAN 9 2015

- d. Number of Copies
- e. Date Mailed
- f. Addressee
- g. Date Unit Rcvd Document (based on return receipt date)
- h. If Tracer Sent (list date of tracer)

5. Return Receipt System. As the central hub for shipping and receiving classified material the MARFORRES Security Management Office will ensure MARFORRES HQs commands and sections shipping or receiving classified material establish a return receipt system to assist in accounting for all classified material and equipment. Acknowledgement of receipt is required for TOP SECRET and SECRET information transmitted or transported in and out of the command. Use OPNAV 5511/10, Record of Receipt, and attach it to the inner cover. The receipt shall contain only unclassified information that clearly identifies the classified information. Retain TOP SECRET receipts for five years and SECRET receipts for two years per reference (b). Failure to sign and return a receipt to the sender may result in a report of possible loss or compromise.

6. Hand Carrying Classified Material. The authority to carry or escort classified material while in a travel status inside the United States and its territories is approved by the MARFORRES Command Security Manager or Deputy Command Security Manager. The Site Security Manager, not located in the MARFORRES Headquarters, may also authorize personnel to carry or escort classified material while in a travel status inside the United States and its territories. Outside the United States and its territories, written authorization from the MARFORRES Command Security Manager or Deputy Command Security Manager, via the chain of command, must be obtained prior to travel. All classified material transported outside the building where is secured must be transported by properly briefed and certified personnel carrying a Courier Card or Courier Letter.

a. The Command Security Manager, Deputy Command Security Manager, MSC or unit Security Manager shall provide written authorization to all individuals escorting or hand carrying classified information. Any of the four following written authorizations may be used, EXCEPT when using commercial

JAN 9 2015

aircraft when a Courier Authorization Letter, Figure 7-1 must be used.

(1) A DD 2501 (Courier Authorization Card).

(2) Authorization statement included on official travel orders.

(3) Authorization statement included on Visitor Requests.

(4) A Courier Authorization Letter (Figure 7-1).

b. Personnel receiving the authorization to hand carry classified material will be briefed by the Security Manager on the provisions of reference (b), and sign a statement acknowledging he/she received and understood the briefing. This statement will be retained by the Security Manager for two years.

c. To hand carry classified material a courier is responsible for the following.

(1) That a completed written inventory of all classified material to be hand carried is conducted prior to the courier's departure and another inventory is conducted upon the courier's return.

(2) The courier and the Security Manager have each signed for the classified material.

(3) The material is properly packaged and safeguarded from unauthorized personnel. A briefcase or courier pouch may not be considered as the outer container in this circumstance.

(4) The courier is liable and responsible for the information being escorted.

(5) The courier understands that the information is not, under any circumstances, to be left unattended.

(6) During overnight stops, classified information is to be stored at a U.S. embassy, military facility, or an appropriately cleared DoD contractor facility.

JAN 9 2015

(7) The information shall not be opened while in a travel status except in the circumstances described in reference (b).

(8) The information shall not be discussed or disclosed in any public place or conveyance.

(9) The courier shall not deviate from the authorized travel schedule.

(10) The courier is responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents) are complete, valid, and current.

(11) There is no assurance of immunity from search by security, police, customs and/or immigration officials on domestic or international flights.

(12) Arrangements for the proper storage of the material at the destination have been made. These arrangements must take into account the time of arrival at the destination to ensure that proper storage facilities will be immediately available for the material. Classified material will not be maintained in hotel rooms, vehicles, or in any unauthorized area. Individuals authorized to hand carry classified material or equipment must take every precaution to prevent the unauthorized disclosure of that information or material per reference (b).

d. When hand carrying classified material inside a building, e.g., from one office space to another, the courier will use an appropriate cover sheet or folder, (e.g. SF 704 SECRET Cover Sheet) to reduce the possibility of unauthorized viewing.

e. When hand carrying classified material outside the building and while in a travel status will be authorized only in those cases where the material is required at the traveler's destination and is not available at that location; or because of time or other constraints the classified material cannot be transported by other authorized means. SIPRNET is the recommended means to access and transmit classified material inside the CONUS and OCONUS.

f. The transport of communication security (COMSEC) equipment, such as the simple key loader (SKL) with Crypto Ignition Key (CIK), ensure the CIK is removed from the device.

JAN 9 2015

This makes the SKL unclassified COMSEC equipment until the CIK is inserted. At which point the SKL will be classified to the level of keying material stored in the SKL. Requirements for transporting COMSEC can be found in EKMS 1B Chapter 5.

g. Transport classified equipment in the following manner:

(1) If the classified equipment is an inaccessible component of a bulky item of equipment, then the equipment may be transported from one point to another without additional wrapping.

(2) If the classified equipment is an item of equipment and the shell of the body is classified, then it shall be draped with an opaque covering that will conceal all classified features. The Security Manager or Security Representative of the storage area from which the equipment was drawn will ensure that this covering is capable of being secured so as to avoid or prevent inadvertent exposure of the item.

(3) Classified material or equipment is not authorized to be carried by privately owned vehicle unless it is being taken from one DoD facility to another DoD facility by direct route, i.e.; point A to point B.

7. Facsimile and Other Electronic Data

a. MARFORRES Command and/or Staff Section personnel with the appropriate security clearance eligibility have the capability to transmit SECRET and confidential documents, via secure fax, to other facilities that also have a secure fax capability. The MARFORRES SCIF will only be used to transmit or receive SCI documents.

b. The MARFORRES Command and Deputy Command Security Manager are responsible for inspecting, designating and segregating specific equipment for classified and unclassified use.

8. Telephonic Transmissions. Only COMSEC devices able to place a secure call are authorized means to discuss classified information by telephone. Classified information will not be transmitted over an unsecure telephone (land line), or cell phone, except as may be authorized on approved secure communication circuits.

JAN 9 2015

(Unit Letterhead)

5510
(SECTION)
Date

From: Security Manager, Marine Forces Reserve (Unit)
To: (Name of person hand carrying)

Subj: AUTHORIZATION TO HAND CARRY CLASSIFIED INFORMATION

Ref: (a) SECNAV M-5510.36
(b) ForO 5510.1_

1. Per the references, you are authorized to escort or hand carry the below listed classified material. You are also authorized to escort or hand carries classified material aboard commercial aircraft in conjunction with the following travel:

a. Employing Agency or Company:

b. Departure Point:

c. Destination:

d. Known Transfer Point:

e. Identification:

(1) U.S. Armed Forces ID Card No.:

(2) Courier Authorization Card No.:

(3) Driver's License No.:

f. Description of material being carried, addressee, sender; package will be signed on its face by the official who signed this letter:

g. Inclusive dates of travel:

h. Expiration Date of Authorization:

Figure 7-1. --Format for Authorization Letter to
Hand Carry Classified Information

JAN 9 2015

2. You are directed to familiarize yourself with the contents of the references prior to your departure.

3. _____, Marine Forces Reserve (MARFORRES) Security Manager, has been designated to confirm this authorization. Telephone number is (XXX) XXX-XXXX.

J. J. JONES
By direction

Figure 7-1. --Format for Authorization Letter to
Hand Carry Classified Information--Continued

JAN 9 2015

Chapter 8

Accountability and Control

1. Basic Policy. The COMMARFORRES has overall responsibility for managing, marking, and controlling classified material. This authority is delegated to the MARFORRES Command Security Manager and Deputy Command Security Manager as the responsible officer and subject matter expert. The MARFORRES Command Security Manager shall ensure that classified information is processed only in secure facilities, on accredited IT systems, and under conditions which prevent unauthorized persons from gaining access.

a. Classified material will be secured in an approved General Service Administration (GSA) container whenever it is not under the direct control of an appropriately cleared person.

b. Areas that manage classified material in an open environment will restrict access and control movement in areas where classified information is processed or stored. These areas will be designated, in writing, by the CO as restricted areas per OPNAVINST 5530.14C, *Navy Physical Security*. All personnel shall comply with the need-to-know policy for access to classified information.

c. Controlled unclassified information (CUI) shall be safeguarded from unauthorized access by the public. Measures shall be taken to protect IT systems which store, process, and transmit such information from unauthorized access.

d. Classified information is the property of the U.S. Government and not personal property. Military or civilian personnel who resign, retire, separate from the DoN, or are released from active duty will not transport classified material outside their command restricted areas, and if an inadvertent transport of classified material does take place the individual shall return all classified information in their possession to the command from which received, or to the nearest DoN command immediately.

e. TOP SECRET material shipped to the MARFORRES HQs will be received by the MARFORRES TSCO. Classified material rated SECRET or below will be received by the Command Security Manager or the Deputy Command Security Manager and hand carried to the appropriate Command or Staff Section.

JAN 9 2015

2. Control Records and Logs. Control records and logs will be manual, automated, or a combination of both as long as the requirements published in this Order are met.

a. Outgoing Registered Mail Log. The outgoing registered mail log or automated file shall contain at a minimum the following information:

- (1) Registered Mail Number
- (2) Serial Number
- (3) Classification
- (4) Number of Copies
- (5) Date Mailed
- (6) Addressee
- (7) Date Unit Received Document (based on return receipt date)
- (8) If Tracer Sent (list date of tracer)

b. Serial Number Control Log. The Security Management Office will maintain logs for the following categories of controlled classified material: U.S. SECRET, NATO TOP SECRET (with separate sections for COSMIC and ATOMAL), NATO SECRET, and U.S. TOP SECRET. The control logs shall contain at a minimum the following information:

- (1) Registered Mail Number
- (2) Serial Number
- (3) Classification
- (4) Registered Mail Number IN (DCS # IN for TOP SECRET logs)
- (5) Date Unit Received Document (based on return receipt)
- (6) Registered Number OUT (DCS # OUT for TOP SECRET Logs)

JAN 9 2015

- (7) Date Out
- (8) Date of Document
- (9) Originator
- (10) Copy Number
- (11) Subject (if classified, write "Classified Subject")
- (12) Disposition (date and destroyed, transferred, etc.)
- (13) Section holding material
- (14) Number of Pages (if TOP SECRET)

3. Incoming U.S. TOP SECRET Material. Incoming U.S. TOP SECRET material will be managed by the TSCO. Minimal amounts of TOP SECRET material will be held within this Headquarters. In most cases, a single copy of each TOP SECRET document will suffice. The TSCO will assign a control number to the material.

a. The following control numbering system will be utilized.

- (1) The first digit is a one.
- (2) The second and third digits reflect the calendar year in which the document was received.
- (3) The fourth, fifth and sixth digits indicate the number of the document for any calendar year.
- (4) For example, 113001 is the first U.S. TOP SECRET document received for the calendar year in 2013.

b. Processing of Incoming U.S. TOP SECRET Material. Upon receipt of a TOP SECRET document, the TSCO assistant will inspect the package for signs of tampering. If none is detected, the package will be opened. If signs of tampering exist, the Command Security Manager, Deputy Command Security Manager, and the MARFORRES Counterintelligence Officer will be notified. When the package is opened, the documents will be separated and verified to match the data appearing on the receipt. The TSCO will sign the document receipt and return to sender. The TSCO will retrieve the TOP SECRET control log, assign the next available control number to the document, and

JAN 9 2015

ensure that the appropriate entries in the logbook are accomplished.

4. Incoming NATO TOP SECRET Material. Control procedures for NATO TOP SECRET material is the same as those used for U.S. TOP SECRET material except that the NATO Control Officer will process all NATO documents. NATO Confidential must be sent by registered mail. NATO TOP SECRET is designated either COSMIC or ATOMAL. The control numbers assigned to NATO TOP SECRET documents are the same as incoming U.S. TOP SECRET .

5. Incoming SECRET Material. Incoming SECRET documents will be controlled and logged by their respective command and/or section custodian with the exception of NATO TOP SECRET, which is under the supervision of the NATO Control Officer.

a. A document serial number will be assigned to the material. The following control numbering system will be utilized.

(1) The first digit is a one.

(2) The second and third digits reflect the calendar year in which the document was received.

(3) The fourth, fifth and sixth digits indicate the number of the document for any calendar year.

(4) For example, 113001 is the first U.S. TOP SECRET document received for the calendar year in 2013.

b. Processing and Handling of Incoming SECRET Material. Upon receipt, only those individuals authorized to receive classified material for their section or unit will sign for the package (refer to Figure 8-2). The package will be inspected for signs of tampering, if none is detected, the package will be opened. If signs of tampering exist, the Command Security Manager, Deputy Command Security Manager and the Counterintelligence Officer will be notified. When the package is opened, the material will be verified against the data appearing on the return receipt. The package will be signed and a return receipt mailed to the sender. Receiving personnel will retrieve the appropriate SECRET control log, assign the next available control number to the document, and ensure that the appropriate entries in the logbook are accomplished. The following information will be also be stamped or affixed to the front cover of the document:

JAN 9 2015

CONTROL NUMBER _____
REC'D DATE _____
COPY _____ of COPIES _____

c. Upon completion, the document will be placed in the appropriate safe and the custodian will be notified.

6. Inventories Frequency and Scope. MARFORRES Commands and Staff Sections that manage classified material will conduct classified material inventories twice annually, at the end of the second and fourth quarters of the Fiscal Year, or in the event of an evacuation or move of all classified material and classified hard drives stored in their area. The Command or Staff Section custodian is responsible for visually inventorying every classified document, media, hard drive, or piece of equipment under their ownership. A current copy of the inventory list will be stored in a GSA certified storage container. A copy of the inventory letter, figure 8-1, will be forwarded to the Command Security Manager verifying the inventory has been completed.

7. Managing Classified Material During Working Hours. MARFORRES Commands and Staff Sections that manage classified material will ensure that classified information is kept under constant surveillance and managed by an authorized person, and covered with classified material cover sheets (SFs 703, 704, or 705) when removed from secure storage.

a. Preliminary drafts, plates, stencils, notes, worksheets, computer disks, hard drives, fax, printer, computer storage media, and other classified items will be protected according to their security classification level. Immediately destroy these items after they have served their purpose.

b. Classified discussions shall not be conducted in public conveyances or places that permit interception by unauthorized persons. Classified material may not be opened or read in any area where it can be seen by unauthorized individuals.

8. End-Of-Day Security Checks. MARFORRES Command and Staff Sections that manage classified material will establish procedures for end of the day security checks, utilizing the SF 701, Activity Security Checklist, to ensure that all areas which process classified information are properly secured. Additionally, an SF 702, Security Container Check Sheet, shall

JAN 9 2015

be utilized to record that classified vaults, secure rooms, strong rooms, and security containers have been properly secured at the end of the day. The SF 701 and 702 shall also be annotated to reflect after hours, weekend, and holiday activities.

9. Classified Meetings. Commands and Staff Sections hosting in-house meetings shall assume security responsibility for the meeting. Security precautions must be taken for conference rooms and areas specifically designated for classified discussions. Commands and Staff Sections hosting meetings outside the command, including those supported by non-U.S. Government associations, shall:

a. Confirm that other means for communicating or disseminating the classified information in lieu of a meeting are inadequate.

b. Confirm that attendance is limited to U.S. Government personnel and/or cleared DoD contractor employees. All attendees shall have an appropriate clearance eligibility and need-to-know.

c. Confirm that security plan has been established specifying procedures for verifying access eligibility, badging procedures, access control procedures, and procedures for storing the classified information.

10. Reproduction of Classified Information. Classified information shall be reproduced only to the extent required by operational necessity unless restricted by the originating agency or for compliance with applicable statutes or directives. Reproduction shall be accomplished by authorized persons knowledgeable of the procedures for classified reproduction in accordance with reference (b). Specific information on reproduction of classified material is covered in chapter 10 of this Order.

JAN 9 2015

(Unit Letterhead)

5510
(SECTION)
Date

From: Section or MSC Unit Site Commander
To: (Rank, Name, EDIPI of Appointee)

Subj: CLASSIFIED MATERIAL INVENTORY LETTER

Ref: (a) SECNAV M5510.36

1. This letter will confirm the classified material inventory of the items listed below.

Item	Serial Number	Description
------	---------------	-------------

2. This inventory will remain in effect until a new classified material inventory is completed.

Signature

Copy to:
SecMgr

Figure 8-1. --Format for Classified Material Inventory

JAN 9 2015

(Unit Letterhead)

5510
G-1
DATE

From: (SCPC, Section)
To: Security Management Office

Subj: ACCESS AND AUTHORIZATION TO RECEIPT FOR CLASSIFIED
MATERIAL FOR (SECTION)

Ref: (a) ForO 5510.1_

1. Per the reference, the following individuals are authorized
to receipt for classified material for the (Section):

NAME	RANK	EDIPI	CLNC	ACCESS
GISH, J. E.	SSGT	xxxxxxxxxx	S	S/NS
DOOR, W. T.	LCPL	xxxxxxxxxx	TS	TS/NS

Signature

Copy to:
Command Security Manager
Each Individual

Figure 8-2. --Format for Access and Authorization
to Receipt for Classified Material

JAN 9 2015

Chapter 9

Security, Storage, and Destruction

1. Basic Policy. COMMARFORRES has overall responsibility for the accountability, control, and destruction of MARFORRES classified material and equipment. This authority is assigned to the MARFORRES Command Security Manager and Deputy Command Security Manager as the responsible officer and subject matter expert. Command and/or Staff Section Chiefs-of-Staff, Directors, OICs, Supervisors, and assigned custodians are responsible for the security and management of classified material located within their areas of responsibility. Commands and Staff Sections will ensure that classified material and equipment is safeguarded and stored as prescribed by the references and this Order.

a. Classified material and equipment will only be used in designated restricted areas where adequate facilities and safeguards are installed to prevent unauthorized persons from gaining access to restricted areas.

b. Personnel will not remove classified material from designated offices or working areas except in performance of official duties and under conditions providing protection required by this Order. Under no circumstances will personnel remove classified material from restricted areas and transport it out of the building to an unsecure area to complete a work project or for personal convenience. Approval to remove classified material from the building for operational purposes must be authorized by the Command Security Manager or Deputy Command Security Manager. Approval to remove classified material will not include permission for overnight storage in any location other than a secure U.S. Government facility, inside a GSA approved container.

c. A courier card or courier letter is required to hand-carry classified material.

d. Classified information will not be discussed with or in the presence of unauthorized personnel. Any personnel that enter a restricted area under escort will be announced and escorted at all times.

e. The required physical safeguards must be in place to

JAN 9 2015

protect classified material, including an electronic security system, a GSA-approved storage container, current SF 700 documents, and a signed inventory of the classified material managed removed is on file with the Command and/or Staff Section Security Manager.

f. Security and storage requirements are developed to provide a uniform guide for establishing security protection for classified material and equipment at the level of security commensurate with the classified material or equipment used in that area. Storage requirements must be tempered and balanced by common sense and security-in-depth. (Security-in-depth is overlapping or reinforcing measures incorporated in such a manner that failure of one security measure will not expose the protected material or equipment to compromise).

g. The requirements specified in the references and this Order represents the minimum acceptable standards. Any questionable area or deficiency in safeguarding and storage procedures will be immediately reported to the Command Security Manager.

2. Physical Security Evaluation (PSE). A PSE will be completed every 12 months on all Limited Access Areas (LAA), Restricted Access Areas (RAA), and Controlled Access Areas (CAA), i.e. Vaults, Strong Rooms, SIPR Rooms, and Open Storage SECRET areas.

a. PSE's will be conducted annually and performed by a trained and certified Physical Security Specialist.

b. The PSE document will be used by the Security Manager to certify the storage of classified material in open storage spaces (up to the level specified in the PSE).

c. A copy of the PSE will be forwarded to the MARFORRES Command Security Manager and the MARFORRES Mission Assurance Program Manager. The PSE will be reviewed and verified annually, and kept on file by the local Security Manager.

d. Should the results of the PSE review indicate that significant changes or modifications to the facility are required, it is the local Security Manager's responsibility to ensure corrective actions are implemented and a request for a new PSE is made to the MARFORRES Command Security Manager. The MARFORRES Command Security Manager will maintain copies of all

JAN 9 2015

PSEs conducted on SIPR Rooms or secure spaces that store classified material.

3. Security Requirements. Security requirements will be developed to provide protection for classified material and equipment at the level of security commensurate with the classified material or equipment used in that area and in reference (e). Storage of classified material marked SECRET or Confidential must be stored in a GSA approved security container. All other applicable physical security requirements must also be met as required by the SECNAV M5510.36B and the MCO P5530.14.

a. Classified material and equipment will only be maintained in facilities or spaces that have been certified with a Physical Security Evaluation (PSE) and designated, by letter, as a restricted area in writing by the Commander or Command Security Manager.

b. Restricted Areas. Different areas require higher degrees of security due to the nature of the work, information and material concerned. Such areas will be designated as RESTRICTED AREAS. Such areas will have warning signs posted at all points of entry and exit. While safeguarding classified material is the basic reason, other valid reasons exist to establish Restricted Areas. These include mission sensitivity, arms, ammunition and explosives, or assets that require additional protection due to risk of theft.

c. Signs and Postings. Signs to restricted areas will read as follows:

WARNING
RESTRICTED AREA - KEEP OUT
AUTHORIZED PERSONNEL ONLY

All words except "WARNING" will be black. The word "WARNING" will be red. All wording will be on red, white, or blue backgrounds, to obtain maximum color contrast.

d. Security and Protection of Work Spaces. All sections, sites and units will implement the security measures necessary to prevent unauthorized persons from gaining access to classified material, including security measures to prevent personnel outside the building and spaces from viewing or

JAN 9 2015

overhearing classified material and discussions. In providing these measures, the following precautions will be taken:

(1) Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible, shall be constructed or covered with materials which provide protection from forced entry. All windows that afford visual observation of classified activities within the facility, shall be made opaque or equipped with blinds, drapes, or other coverings.

(2) Personal Electronic Devices (PED) such as cell phones, Blackberries, radios, or recording devices will not be allowed in restricted areas where classified material is stored, received, or sent via a hardline connection or wireless signal. Signs to restrict these electronic devices will read as follows: WARNING: NO CELL PHONES OR ELECTRONIC RECORDING DEVICES (Turn Off and Store in designated storage area before entering).

e. Security during Working Hours. During working hours the following precautions will be taken to prevent either visual or audible access to classified information by unauthorized personnel:

(1) When classified material is removed from the security container, it will be kept under constant surveillance by appropriately cleared personnel. An appropriate cover sheet (SF 703, 704, 705), will be placed over all classified material to prevent visual access. When not in use the material will be returned to an approved security container for safeguarding;

(2) Classified material will not be left unattended for any reason.

(3) Items containing classified information, will be protected in the same manner as prescribed for the highest level of classified material they contain. After use, such items will either be properly destroyed or secured in an approved GSA security container.

(4) Protect classified material by turning computer monitors away from public view and cover or store items not in use.

JAN 9 2015

(5) Ensure that all hard copy and media classified material has been properly stored in a GSA approved container, or destroyed.

f. Security Checks. Random checks will be performed hourly throughout the facility. During working hours the following security checks will be performed:

(1) Supervisors will establish a regular security check of each office and working space at the end of each working day to confirm that all classified material is properly secured. The Standard Form (SF) 701, Activity Security Checklist will be used to record daily security checks. The SF 701 will be posted inside the entry door of every restricted area that processes or stores classified material.

(2) An integral part of the security check system consists of securing all vaults and security containers used for the storage of classified material. The SF 702 will be completed by the designated individual inspecting that security container. SF 702, Security Container Check Sheets, will be posted on the outside of each security container and used to record daily security checks of safes and vaults. SF 701 and 702 will also be used to reflect after hours, weekend, and holiday activities.

(3) Safes, vaults, and security containers will be locked by the responsible custodians and double checked. (The spin dial of the combination lock must be rotated at least four complete times in the same direction when securing the container).

4. Storage Requirements

a. Security Containers. Only GSA approved security containers will be utilized for the storage of classified material and equipment. GSA approved field safes or portable containers, if utilized, will be rendered non-portable by securing them to a permanent fixture while in a garrison environment.

(1) A GSA security container will be used for the storage of classified material, and the most sensitive material.

JAN 9 2015

(2) A Maintenance Record for security containers and vault doors (Optional Form 89) will be maintained for each security container used for the storage of classified material. This form will be placed inside the control drawer of each container.

(3) Security containers will be inspected quarterly, and all inspections and repairs will be annotated on the Form 89.

(4) Security containers used for the storage of classified material will have a current, and properly completed, Security Container Information Form (SF 700) attached to the inside of the control drawer. The SF 700 is used to maintain a record for each security container, vault, or secure room door showing the location of each, the names, and telephone numbers of the individuals having knowledge of the combinations and who are to be contacted in the event the security container, vault or secure room is found open and unattended.

(5) Valuables will not be stored in the same container used to safeguard classified material.

(6) There shall be no external markings revealing the classification level of information being stored in a specific security container, vault, or secure room. Priorities for emergency evacuation and destruction shall not be marked or posted on the security container.

(7) Safes and security containers that are not being utilized for storage of classified material will have a sign attached to it which reads, "THIS CONTAINER IS NOT USED FOR THE STORAGE OF CLASSIFIED MATERIAL."

b. Vaults and Strong Rooms. Storage requirements for large amounts of classified material, or odd-shaped or bulky material, can be met in many instances by vaults or strong rooms. They must conform and be built to the standards specified in DoD 5200.08-R, OPNAV 5530.14E and this Order. Vaults or strong rooms may not be used for storage of classified material unless a current PSE has been conducted and the space meets the specific requirements outlined in SECNAV M5510.36B and the MCO P5530.14.

c. Combination and Cipher Locks. To ensure the effectiveness of combination locks and cipher locks, the combination will only be given to those personnel whose official

JAN 9 2015

duties demand access to the container. Combinations will be changed when any of the following instances occur:

(1) When containers and locks are first placed into service.

(2) When an individual knowing the combination no longer requires access unless other sufficient controls exist to prevent access to the lock.

(3) When the combination has been subject to possible compromise or the security container has been discovered unlocked or unattended.

(4) When the security container is taken out of service.

(5) The same combination will not be used for more than one container in any one classified material storage area.

(6) To prevent a lockout, two different people should try the new combination at least three times before closing the container or vault door.

(7) Records of combinations will be annotated and sealed in the Security Container Information Form, SF 700.

(8) Combinations have the same classification as the material they protect; therefore personnel that do not have the appropriate security clearance eligibility will not have access to the combination or be able to change combinations.

d. Setting Spin Dial Combinations. Combinations for security containers must be annotated on a Security Container Information Form (SF 700). To assign a lock combination to the security container, fill out the SF 700 using the following steps.

(1) Part 1 of the completed SF 700 on an interior door of the security container, vault, or secure room door.

(2) Fill out Parts 2 and 2A of the SF 700 with the combination code and the highest classification level.

(3) Both copies will be complete in ink. The envelope will be sealed in lamination to prevent tampering. Store Parts 2 and 2A in a GSA approved container in a secondary location.

JAN 9 2015

(4) MARFORRES Commands and Staff Sections will store copies of the SF 700 in the G-3 COC with a second copy secured in the MARFORRES Security Management Office safe.

e. Supplemental Locks and Access Control. Lock requirements can be found on the DoD Lock Program site at http://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html or by calling the DoD Lock Program Technical Support Hotline at (800) 290-7607. DoD 5200.08-R and OPNAV 5530.14E list specific lock, alarm, and physical security requirements.

(1) STU-III CIK. CIK "Keys" will not be left in the unit's overnight. CIK's will be removed from and secured away from the STU-III when not in use. CIK's are not required to be secured in a GSA container. For transport of COMSEC equipment, such as the SKL with CIK, ensure the CIK is removed from the device. This makes the SKL unclassified COMSEC equipment until the CIK is inserted. At which point the SKL will be classified to the level of keying material stored in the SKL.

(2) Key Sector Vector (KSV)-21 Cards. KSV-21 cards associated to a Secure Telephone (STE) will not be left in the unit's phone unattended. When the card is disassociated from the phone, the KSV-21 card will need to be stored in an alternate office away from the STE phone when not in use. KSV-21 cards are not required to be secured in a GSA approved safe.

(3) Electrical and Mechanical Locks. Cypher and Simplex locks do not afford the degree of protection required for classified material storage. They will not be used as the primary means to safeguard classified material. However, such locks are authorized as traffic control devices for restricted areas and secondary locking devices, and can be used to secure a space that locks small amounts of classified material in a GSA approved container. Master keys are supervised by the MARFORRES Facilities Building Manager and will be managed and inspected by the Command Security Manager.

(4) Electronic Security Systems (ESS). An ESS consists of one or more of the following subsystems: Intrusion Detection System (IDS), Closed Circuit Television (CCTV), Motion Detectors, and Access Control System (ACS). The ESS is continuously monitored by appropriately cleared personnel and all trained law enforcement personnel respond to all annunciated alarms. The monitoring stations are located in a secure area

JAN 9 2015

and all components are tamper protected in accordance with Marine Corps Electronic Security System (MCESS) guidelines. Shunting or masking an alarm signal is unauthorized. All IDS systems that are used as supplemental control for vaults or secure rooms/areas containing SIPRNet assets will be checked for proper operation by the Facilities Building Manager as follows:

(a) Maintenance and functionality checks will be conducted and logged on a periodic cycle at least every 90 days.

(b) Valid tests in accordance with best practices using government or industry standards and tools will be used to conduct the checks.

(c) Written procedures will be developed for tests of each sensor type in use at the site.

(d) Results of testing will be maintained on file for at least 180 days.

(e) For more information regarding electronic security systems refer to SECNAV M5510.36B, Chapter 10-16 and MCO 5530.14. Questions concerning requirements for Electronic Security Systems and access control should be addressed to the MARFORRES Command Security Manager.

5. Repairs and Modifications to Security Containers. Repair of a security container approved for storage of classified material shall only be done by appropriately cleared or continuously escorted personnel. Notify the local Security Manager when any lockout or repair is required. More specific information on repairs is found in reference (b), chapter 10.

6. Methods of Destruction. Classified material and equipment will be destroyed by the methods outlined below and in chapter 10 of reference (b). All units that work with classified material will be equipped with an authorized shredder or destruction equipment that meets the requirements for the destruction of the classified material. Classified material will be destroyed only by authorized means and by personnel cleared to the level of the material being destroyed. Hard drives will not be downgraded, upgraded, or declassified. All hard drives will be transported to the MARFORRES Security Management Office to be degaussed and destroyed in accordance with NSA/CSS Storage Device Declassification Manual 9-12 and reference (b).

JAN 9 2015

7. Destruction Procedures for Classified Material. Listed below are the procedures for destroying classified material.

a. All classified material not in use will be inventoried annually and destroyed. Satellite locations will request authorization from the MARFORRES Command Security Manager or Deputy Command Security Manager before destroying buck tagged items. A completed OPNAV 5511/12 form will be sent to the Command Security Manager.

b. Classified material will be destroyed only by authorized means by personnel cleared to the level of the material being destroyed.

c. Documents up to SECRET will be shredded utilizing a DOD/NSA approved cross-cut shredder, in accordance with reference (b).

d. All MARFORRES Commands and Sections will establish a "clean-out" day at least twice a year to focus specific attention and effort on the disposition of unneeded classified material.

e. Destruction of TOP SECRET material requires two per integrity, two witnesses, and a record of the destruction.

f. All EKMS/COMSEC material will be delivered to the EKMS Manager for proper destruction and disposal.

g. Record the destruction of TOP SECRET material on an OPNAV Form 511/12 (Classified Material Destruction) or in a destruction log. Destruction records include complete identification of the material, number of copies destroyed, and the date of destruction. Destruction records for TOP SECRET will be maintained for a minimum of five years.

8. Destruction Procedures for Classified Hard Drives. Hard drives will not be downgraded or declassified. Hard Drives will be turned into the Security Management Office to be degaussed and destroyed as per NSA/CSS Storage Device Declassification Manual 9-12. Hard drives will be destroyed using the following procedures.

a. Remove all labels or markings that indicate previous use or classification.

JAN 9 2015

b. Remove the hard disk drive from the computer chassis or cabinet, and remove any mounting brackets.

c. Degauss the hard drive with an NSA/CSS certified degasser.

d. Physically crush or punch the disk drive after it is erased in a degasser.

e. Destruction will be recorded in a log, and records will be maintained for a minimum of two years.

f. Dispose or recycle erased and destroyed disk drive.

g. The degausser will be periodically tested and certified as required by the manufacturer. Documentation of this testing and certification will be maintained by the Command Security Manager.

9. Emergency Action Plan (EAP). Establishing a working EAP for the control and security of classified material is a DoD mandated requirement. In an emergency involving the danger of loss or compromise of classified material or equipment, the importance of initiating the early removal or destruction of classified material cannot be overemphasized. All personnel shall be indoctrinated in the procedures for the emergency removal and destruction of classified material as stated in the command EAP. When required, the senior person present will initiate the necessary action without waiting for specific orders from higher authority. A periodic review (bi-annually) of classified material holdings is essential in order to identify classified material that is no longer needed, and to reduce the amount of material that must be moved or destroyed in an emergency.

a. Every Command and/or Staff Section that stores classified material is required to develop an EAP for the protection of classified material in case of natural disaster, civil disturbance or enemy action. The Security Manager is responsible for developing an EAP that includes all MARFORRES Commands/Sections that manage classified material, and will coordinate the CMS/EKMS and SCIF EAPs to ensure unity of effort. The EAP will provide for the protection of classified information in a way that will minimize the risk of injury to personnel and property.

JAN 9 2015

b. Classified Material EAP. In the event of a predicted catastrophic weather event or imminent threat the Security Manager will coordinate storage of all hard copy classified documents, classified equipment, hard drives, and computers that are not stored in the EKMS Vault or the SCIF. The identified classified items will be inventoried and stored as per this Order or the reference (b). Classified material located on the MARCORSPTEFAC will be inventoried by the classified material manager and stored in a GSA approved storage container. The Security Management Officer (SMO) will maintain a list of all classified material evacuated, relocated, or destroyed.

c. Preparing for Emergency and Evacuation. MARFORRES Security Representatives and assigned personnel will ensure the following items are maintained quarterly in preparation for emergency evacuation.

(1) Store only the minimum amount of classified material required for operational purposes.

(2) Destroy excess material in accordance with reference (b), using appropriate disposal means.

(3) Store classified material in GSA approved, secure storage containers.

(4) Complete classified material inventories twice annually, or when personnel authorized to handle the material transfer.

(5) Ensure combinations to all vaults, safes, and secure spaces are recorded on SF 700. Store one copy in the COC and one copy with the Command Security Manager.

d. In the Event of an Evacuation. In the event of an emergency, such as fire, natural disaster, civil disturbance, or terrorist attack requiring evacuation of personnel, Security Managers and Representatives will manage and maintain classified material as required per reference (b). Upon receipt of evacuation instructions.

(1) Classified material will be secured in secure storage vaults or containers before evacuation.

JAN 9 2015

(2) The security system will be armed and X09 locks will be engaged.

(3) The supervisor will notify the Command Security Manager and the Marine Corps Police of the emergency, and ensure that classified material is secured.

10. Emergency Destruction. All deployed commands must address in their EAP the emergency destruction of classified information. Classified material will be destroyed in accordance with this Order and reference (b). Procedures for the emergency destruction of SCIF and COMSEC material will be prepared and implemented as follows:

a. The SSO will prepare an EAP per the M1 Manual and reference (b).

b. The EKMS Manager will prepare an EAP for all COMSEC material per current EKMS directives. A copy will be provided to the MARFORRES Command Security Manager.

c. The SSO and EKMS Manager will confirm with the Command Security Manager that their respective EAP's are up-to-date and in place.

JAN 9 2015

Chapter 10

Dissemination, Reproduction, and Photography of Classified Material

1. Basic Policy. COMMARFORRES has overall responsibility for the dissemination, reproduction, and photography of classified material originated or received by the MARFORRES commands and Staff Sections. This authority is delegated to the MARFORRES Command Security Manager as the responsible officer and subject matter expert for dissemination, reproduction and photography of classified material, and ensuring appropriate security guidelines and provisions are followed. Site Commanders and/or OICs are responsible for all dissemination, controlling reproduction, and photography of classified material within their commands.

2. Dissemination. Classified information originated in a non-DoD department or agency shall not be disseminated outside the DoD without the consent of the originator except where specifically permitted (also known as the "third agency rule").

a. TOP SECRET. TOP SECRET information originated within the DoD shall not be disseminated outside the DoD without the consent of the originator or higher authority.

b. SECRET and Confidential. Unless specifically prohibited by the originator, SECRET and Confidential information originated within the DoD may be disseminated to other DoD components and agencies within the executive branch of the U.S. Government.

c. NATO. DoN documents which incorporate NATO information do not require transmission through NATO channels.

3. Reproduction Controls. It is the policy of this Command that reproduction of classified material will occur only when absolutely necessary and then only when specifically authorized as detailed below. The term "reproduction" will include reproduction machines, i.e. copy machines, scanners, and/or any other hardware able to record and store images or data.

a. TOP SECRET. TOP SECRET material will not be reproduced or photographed without written approval by the originator's

JAN 9 2015

higher authority and the Command's TSCO. Records of the number and distribution of all reproductions of TOP SECRET documents will be maintained for a period of two years. Commands/Sections requiring reproduction of TOP SECRET material will submit a written request to the TSCO.

(1) The TSCO will initiate action to obtain reproduction approval from the document originator.

(2) Once approval is obtained, the TSCO will ensure two TOP SECRET (TS) cleared personnel perform the reproduction. When reproduction is accomplished, the TSCO will log in, mark, and control all copies.

(3) The TSCO will retain TOP SECRET document reproduction records (inventories, approval letters, logs, etc.) for two years.

b. SECRET Material or below. Classified material rated SECRET or below that is controlled and has been assigned a serial number will be reproduced only by the Command and/or Staff Section managing that specific piece of classified material. Records of the number and distribution of all reproductions of SECRET and Confidential documents will be maintained for a period of two years.

4. Reproduction Equipment. Equipment designated for classified material reproduction will be located in a secure restricted area where reproduction can be controlled and precautions taken to prevent viewing of the material by unauthorized personnel.

a. A sign will be located on or near the reproduction machine which states "THIS MACHINE MAY BE USED FOR REPRODUCTION OF CLASSIFIED MATERIAL UP TO AND INCLUDING SECRET."

b. Classified material reproduction equipment will be marked with a classified sticker and separated at least five feet from unclassified material reproduction equipment.

c. Upon completion of the reproduction of classified material, personnel will place a blank sheet of paper on the machine and reproduce it no fewer than three times. This will help ensure that no images are left on the machine. If a malfunction or paper jam occurs during reproduction of

JAN 9 2015

classified material, extreme care should be taken to ensure that classified material is not left in the paper path.

d. Machines that are not authorized for reproduction of classified material will be marked with an "unclassified" sticker and segregated from classified equipment and material

e. Equipment used for reproduction of TOP SECRET material will be located only in a secure vault certified and approved for TOP SECRET storage.

5. Photography Controls. The MARFORRES Command Security Manager or Deputy Command Security Manager will be in coordination with the Public Affairs Officer (PAO) has overall responsibility for controlling photography and ensuring appropriate security guidelines and provisions are maintained. The MARFORRES Site Security Manager, in coordination with their Commander, are responsible for ensuring appropriate security guidelines for their respective Commands. Photography and videography performed inside a MARFORRES HQs restricted area, or open storage SECRET or TOP SECRET area, must be authorized by the MARFORRES Command Security Manager.

a. Photographs by DoD Personnel. Marine Corps Public Affairs personnel and Combat Camera personnel are authorized to act as official photographers and escorts for MARFORRES sanctioned photography and videography events.

b. Marine Corps Public Affairs and/or Combat Camera personnel are authorized to bring cameras into the command are subject to any restrictions imposed, by the Command and/or Staff Section, for the protection of classified material.

c. Photographic equipment is not authorized in the SCIF, or areas designated as Open Storage SECRET or Restricted Areas.

6. Control of Personal Electronic Devices (PED) and Recording Systems. Absolutely no PED, i.e. two way radios, cell phones, Personal Digital Assistance (PDA), iPods, Flash Drives, Blackberries or devices, that will record or download sound or information, will be allowed in any SIPR room, or open storage, restricted area where classified material is processed or stored.

a. Personnel will not be allowed to bring PEDs or voice recording equipment to any classified briefings.

JAN 9 2015

b. Non-approved audiovisual equipment is not allowed in the SCIF or any area that has been designated as a restricted area or open storage SECRET area.

JAN 9 2015

Chapter 11

Access Control and Visitor Control

1. Basic Policy. This chapter provides guidance for access control and visitor control procedures for classified conferences, meetings, and exercises in unclassified and Restricted Areas. COMMARFORRES has overall responsibility for the Access Control Program for MARFORRES Commands and Staff Sections. This authority is delegated to the MARFORRES Command Security Manager and Deputy Command Security Manager. The MSCs will be responsible for establishing visitor control procedures within their respective commands as directed by this Order and reference (b). A visitor is any person who is not a CAC Card holder assigned to MARFORRES, MARFORNORTH or MARCORSPTFAC New Orleans.
2. Visitor Access Control. Any visit involving access to classified information requires a designated action Officer or Security Representative to submit a Visit Request to the Command in order to properly verify security clearance eligibility and grant access to classified material. All Visit Requests will be sent from Security Manager to Security Manager via the JPAS.
 - a. The Security Manager is responsible for preparing and submitting a Visit Request in JPAS for any visiting personnel that requires access to classified information.
 - b. MARFORRES personnel visiting other Commands, Agencies, or Companies will submit requests to the MARFORRES Security Management Office one week in advance of the proposed visit in order to give the MARFORRES SMO sufficient time to process the visit request.
 - c. Visitors who are authorized access to classified material will present their CAC card as identity verification.
 - d. The Security Manager will maintain a file of all visit requests for a period of two years.
 - e. Personnel entering the MARCORSPTFAC, New Orleans must have a CAC Card and a MARCORSPTFAC Access Badge. All visitors must check into the Visitors Center to be approved for entry. Visitor entry will be limited to those individuals who have the proper identification (CAC Card, Retired ID, or Driver's License

JAN 9 2015

and a command sponsor). Personnel visiting the MARCORSPTFAC, New Orleans must contact the MARFORRES Security Managers office for visitor request requirements.

f. Security clearance eligibility annotated on original orders or hand carried JPAS pages or clearance letters are not authorized. Clearance certification can be forwarded via Official Letter from a Government Agency or Company Facility Security Officer (FSO) if JPAS is not available. The form can be emailed, in a PDF format on encrypted email, or faxed to the Security Management Office of the site to be visited.

3. Visits by Flag/General Officers and their Civilian Equivalents. As a matter of courtesy, Flag Officers, General Officers, and their civilian equivalents are considered VIPs and will be identified and cleared in advance. VIP staff personnel will coordinate visits and entry into the MARCORSPTFAC with the MARFORRES Protocol Officer and the Command Security Manager.

4. Meetings. Meetings are defined as a gathering of personnel for the purpose of discussing or presenting information. Classified information will not be disclosed at meetings, conferences, or other gatherings unless adequate security measures are taken to control access to the information and prevent its compromise. The MARFORRES Command Security Manager or Deputy Command Security Manager will be notified and consulted before any classified meetings are conducted outside of designated secure areas. The classification of meetings cannot be changed once the meeting has begun (e.g. meetings cannot "go secure"). Notification and preparations will be in made in sufficient time to ensure all appropriate security measures are in place prior to presentation of classified material.

a. A classified meeting conducted by an MARFORRES Command and/or Staff Section must comply with the Order, SECNAV M5510.30B and reference (b).

b. The Command and/or Staff Section conducting a classified meeting will assign a security sponsor and be responsible for ensuring that the following security requirements are met:

(1) Areas in which classified information is to be discussed must afford adequate security against unauthorized access and disclosure.

JAN 9 2015

(2) Adequate classified material storage facilities will be available.

(3) Attending personnel have the clearance access eligibility and an approved Visit Request on file in JPAS.

(4) Admittance is limited only to those on an approved access list and then only upon proper identification.

(5) Each person who will disclose classified information has been notified of the security limitations which must be imposed because the level of access authorized, the need to know, and the physical security conditions.

(6) Provisions have been made to control and safeguard classified material.

(7) Sessions are monitored to ensure discussions are limited to the level authorized.

(8) A thorough walk through inspection is completed before and after the meeting.

JAN 9 2015

Chapter 12

Personnel Security Investigations and Security
Clearance Access Eligibility

1. Basic Policy. COMMARFORRES has overall responsibility for the Personnel Security and Investigations Programs for MARFORRES Commands and Staff Sections. This authority is delegated to the MARFORRES Command Security Manager and Deputy Command Security Manager as the responsible officer and subject matter expert. MSC Security Managers will be responsible for adhering to personnel security requirements within their respective commands as directed by this Order and SECNAV M5510.30.

2. Security Indoctrination. All personnel will receive security indoctrination and orientation brief that will give them a thorough understanding of what classified information is and why/how classified information is safeguarded. Military members will receive an indoctrination brief upon check-in through the Security Management Office. The Security Manager will ensure that all Military, Civilian, and Contractor personnel reporting to a MARFORRES Command receive a security orientation brief that covers the requirements of maintaining a security clearance, protecting classified material, and the importance of Security Awareness and Security Programs as a whole.

a. The security indoctrination process is a critical function of the check-in and check-out process. In performing the check-in and check-out process all personnel will be updated in JPAS and a personnel security folder will be created that includes the following:

- (1) A completed and signed Form 5521; left side page (1).
- (2) The Security Orientation/Awareness Briefing, left side of page (2).
- (3) The NDA SF312 located on the left side of page (3).
- (4) NATO In-Brief/Out-Brief, left side of page (4).
- (5) Copy of JPAS page, right side of page (1).

JAN 9 2015

(6) Military copy of orders; Civilian personnel copy of the Position Description (PD); Contractors copy of contract; right side of page (2).

3. Investigative Requirements for Security Clearance Access Eligibility. A Personnel Security Investigation (PSI) is conducted to gather information pertinent to these determinations. Clearance access eligibility will not be approved unless a favorable personnel security determination. The term "PSI" refers to an information gathering inquiry, where specified information is collected from specified sources to support eligibility determinations as per SECNAV M5510.30.

a. TOP SECRET/SCI (TS/SCI). The investigative basis for a TOP SECRET clearance eligibility is a favorably adjudicated SSBI Periodic Reinvestigation (SSBI-PR) or Phased Periodic Reinvestigation (PPR). For those who have continuous assignment or access to TOP SECRET material, the SSBI must be updated every 5 years by a PPR.

b. SECRET /Confidential. The investigative basis for a SECRET or Confidential clearance is a favorably adjudicated National Agency Check with Local Agency and Credit Checks (NACLIC). For a SECRET clearance, the investigation is updated every 10 years by means of a new NACLIC investigation for a SECRET Clearance.

c. NATO. The investigative basis for assignment to a NATO billet is a favorably adjudicated SSBI-PR, PPR, Access National Agency Check with Inquiries (ANACI), NACLIC, or adjudicated Entrance National Agency Check (ENTNAC) depending on the level of clearance eligibility and access the billet requires. However, the investigation must have been completed within the five years preceding the assignment no matter what level of access is required. An individual with a Temporary (Interim) SECRET clearance cannot be granted NATO Access.

d. Other Investigative Requirements. The Command Security Manager or Deputy Command Security Manager is required to verify that the individual requesting a clearance is assigned to an MOS, or position that requires a security clearance prior to approving the clearance request. Individuals requesting a security clearance must be U.S. citizens. Personnel that are not eligible for a security clearance will not be allowed into a restricted area or remain in a position requiring security

JAN 9 2015

clearance access eligibility. Military personnel are required to have a minimum of a NACL/SECRET clearance. Only U.S. Citizens (Native or Naturalized) are eligible for a security clearance. Foreign Nationals will first initiate a request through the Foreign Liaison Office via Mission Assurance and must be approved by the Command Security Manager any before access eligibility is authorized. Military personnel are required to have a minimum of a NACL/SECRET clearance. Specific personnel security investigative requirements can be found in reference (a), Chapter 6.

4. Security Clearances and Investigations. COs have ultimate authority over who may have access to classified information under their control. Therefore, each CO should first conduct a thorough review of all billet identification codes, Military Occupational Specialty (MOS), and Civilian PD under their control to determine whether access to classified information is essential to accomplish the mission. The MARFORRES Command Security Manager and the Deputy Command Security Manager maintains a roster of required clearances for each T/O and line number at MARFORRES Headquarters. Commands that are assigned new Marines should check with the MARFORRES Command Security Manager or Deputy Command Security Manager on clearance requirements. Clearance and access eligibility is based on MOS and position requirements. No person will be given access to classified information or be assigned to sensitive duties unless a favorable personnel investigation has been made regarding his/her loyalty, reliability, and trustworthiness. Access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission, and will be based on eligibility and need-to-know.

a. Determining Level of Access. A review of the minimum level of access for each billet should be conducted. The level of access authorized will be limited to the minimum level required to perform assigned duties.

b. Responsibility for Requesting PSI. Security Managers are responsible for requesting PSIs on assigned personnel, with the exception of those personnel requiring access to SCI. PSIs for SCI access will be forwarded to the MARFORRES SSO for processing.

c. Initial Determination. The initial determination will be based on a local records check and review by the Security Manager. The PSI, that is appropriate to the level of security

JAN 9 2015

clearance access required, will be imitated via EQIP and routed through OPM and DoD Central Adjudication Facility (CAF). Requests for PSIs will be kept to an absolute minimum and based on the individual's MOS or employee's PD.

d. Before initiating an investigation Security Managers should consult SECNAV M5510.30 and this Order, and determine:

(1) That the individual does not already have a valid investigation which would satisfy the requirements (see paragraph 2 below);

(2) Validate that the individual is a U.S. citizen;

(3) Verification of the individual's date and place of birth.

e. Verification of Investigation. The JPAS is the only acceptable form of verification of personnel's current security clearance eligibility.

f. PSIs will not be requested for individuals with less than one year of active service.

g. MARFORRES personnel will request PSIs on the MARFORRES Share Portal Security Portal Page using the Clearance Request Form.

h. All PSIs will be processed by a MARFORRES Security Specialist using EQIP Direct and approved by the Command Security Manager or Deputy Command Security Manager.

5. Security Clearance Request and Submission. MARFORRES personnel will submit for a security clearance through the MARFORRES SharePoint Security Portal page, at <https://sharepoint.marforres.usmc.mil/Security/SitePages/Home.aspx>

a. First complete the Clearance Request Form on the MARFORRES SharePoint Security Portal.

b. Local Security Manager uploads completed Clearance Request Form on the MARFORRES SharePoint Security Portal page, <https://sharepoint.marforres.usmc.mil/Security/SitePages/Home.aspx>. If, for some reason, your Clearance Request Form is disapproved the requestor will be notified.

JAN 9 2015

If, for some reason, your Clearance Request Form is disapproved the requestor will be notified.

c. The requesting Command will be notified of approval by email along with the instructions on how to access the EQIP website via the EQIP login to complete your Personnel Security Questionnaire (PSQ) submission paperwork.

d. Complete your EQIP Login and fill in your personal information on the PSQ.

e. Sign and forward the signature pages to your point of contact at the MARFORRES Security Management Office. Remember to print a copy of your signature pages.

f. Submit your fingerprints using an Office of Personnel Management (OPM) certified electronic fingerprint scanner. If you do not have access to an electronic fingerprint scanner contact the MARFORRES Security Management Office.

g. OPM will accept the request and forward the investigation results to the DoD CAF.

h. DoD CAF will investigate and notify the MARFORRES Security Management Office via JPAS when the individual's security clearance has been adjudicated.

i. Submitting PSQs through JPAS is prohibited. All PSQs must be submitted via EQIP Direct through the Security Management Office.

6. Requests for Additional Information. Periodically, a completed investigation being adjudicated at DoD CAF may contain information that requires expansion. In these cases DoD CAF will forward additional investigative forms, Letters of Inquiry (LOI), to the requesting command for the requesting individual to complete and return to DoD CAF, in a timely manner, for final adjudication. In some cases DoD CAF will notify the Command via the JPAS Notifications tab of any issues or questions related to the investigation. The notification process for an LOI package must be coordinated by the appropriate Security Manager, or the MARFORRES SSO, if related to SCI. Notify the MARFORRES Command Security Manager or Deputy Command Security Manager of any issue, change, or questions concerning an individual's security clearance eligibility.

JAN 9 2015

7. Granting Final Clearance Eligibility. DoD CAF is the sole authority for granting final security clearance eligibility for DoD personnel.

8. Temporary (TEMP/INTERIM) Clearance Access Eligibility. Temporary clearance access eligibility is granted to personnel initiating and initial personnel security investigation and approved by the MARFORRES Command Security Manager or Deputy Command Security Manager on a temporary basis. The approval for TEMP access is based on a local records check, with a full completion of PSI requirements that are approved by OPM.

a. TEMP Access may be granted only after the following:

(1) Command and/or Staff Section submit a Security Clearance Request Form following the process described in this chapter, paragraph 5.

(2) A favorable review of the completed PSQ.

(3) Local records and background check does not reveal any derogatory information.

(4) The EQIP investigation submission has been received and approved by OPM.

(5) In the case of TEMP TOP SECRET clearance access, a favorably adjudicated investigation must already be on file at DoD CAF. TEMP TOP SECRET access is effective until final adjudication is made.

9. Access Eligibility. Access eligibility for personnel to gain any access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and will be based on the individual's need-to-know. Additionally, the level of access authorized will be limited to the minimum level required to perform the assigned duties. No one has a right to have access to classified information solely because of rank, position, or security clearance eligibility.

a. A NDA Form (SF 312) must be executed by all personnel prior to gaining access to classified information. In addition to the NDA, individuals who are entrusted with access to TOP SECRET information and/or indoctrinated into Special Access

JAN 9 2015

Programs must complete a "Personnel Attestation" prior to gaining access to TOP SECRET information.

b. The Security Manager will ensure that the individual is given a security orientation briefing and that all requirements have been fulfilled before granting access to classified material.

10. Access List. Command and/or Staff Section Chiefs-of-Staff, Directors, OICs, or designated Military and Civilian personnel are responsible for verifying and approving the list of personnel (Access Roster) that are authorized to access an Open Storage SECRET Area, CAA, Restricted Area, and/or a Special Access Area (SAA) that is under their authority.

a. The Access List, reviewed and approved by the designated individual in that Command and/or Staff Section and the Command Security Manager, shall be prominently displayed on the inside of the Restricted Area's main door. The Command Security Manager is the approval signature on all Access Lists in the MARFORRES HQ.

b. Access Roster Required Information. The following information will be present on all access rosters: Name, Rank, Date, and Level of Clearance Access.

11. One-Time Access. An urgent operational or contractual emergency may arise for cleared personnel to have one-time or short duration access to classified information at a higher level than that for which they are eligible. Only a Flag Officer, General Officer, a General Courts Martial Convening Authority, or equivalent Senior Executive Service (SES) civilian may grant one-time access, after coordination with the MARFORRES Command Security Manager or Deputy Command Security Manager. Therefore, for compelling reasons that are mission critical, an individual may be granted access at one level of classification higher than their current clearance access eligibility, subject to the terms and conditions outlined in reference (a).

12. Access by Reserve Personnel. Reserve personnel in an "active status" may be granted access as necessary provided they hold the appropriate clearance. A record of access granted should be maintained by the Security Manager and properly initiated in JPAS. Specific information can be found in Chapter 9 of reference (a).

JAN 9 2015

13. Suspension of Access. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the CO or I-I may decide to suspend access. Suspension of access for cause is only used as a temporary measure. DoD CAF will make the final determination on suspension of clearance access.

a. MARFORRES Chiefs-of-Staff, Directors, or OICs will inform the MARFORRES Command Security Manager or Deputy Command Security Manager of any action or incident that may impact an individual's ability to maintain a security clearance.

b. When an individual's security clearance access has been suspended, the Command Security Manager will:

(1) Advise the individual of the suspension to include a brief statement of the reason.

(2) Initiate an Incident Report in JPAS with suspension of access.

(3) Take steps to ensure that the individual's access is removed from any Secure Access List, that all access control certificates are removed from any access badge or CAC Card, and that all coworkers are notified of the suspension.

(4) Notify the Command and/or Staff Section Security Managers, Security Representatives, and supervisors so that all combinations to classified storage containers are changed and that all access to classified material has been recovered from the individual.

(5) For Marines with MOS of 02XX or 26XX, notify MARFORRES SSO and forward the same information provided to DoD CAF.

c. Chiefs-of-Staff, Directors, and OICS of MARFORRES Command and/or Staff Sections will ensure that the MARFORRES Command Security Manager or Deputy Command Security Manager is aware of any individual with a pending investigation, pending disciplinary action, active administrative discharge board, pending release from active duty under "Other Than Honorable conditions, or placed in the care of a doctor for behavior or mental health issues reasons."

JAN 9 2015

14. Termination of Access. Access to classified information and/or equipment will be removed from JPAS and access control systems when:

a. The individual no longer requires need-to-know or possession of classified information or equipment in order to accomplish their assigned mission.

b. The individual transfers, separates from service, or retires.

c. The individual becomes ineligible to maintain a security clearance.

15. Investigation Requirements for Access to Sensitive Compartmented Information (SCI). The SSBI is the standard investigative prerequisite for access to SCI and a civilian's assignment to critical-sensitive/special sensitive positions. The MARFORRES SSO is responsible for SCI, and the SSO's responsibilities include the management of SCI security clearances and the approval of access to SCI material.

a. Individuals with a valid mission requirement and need-to-know shall conduct a pre-screening interview with the SSO. Favorable pre-screenings are processed by the SSO for a SSBI.

b. Access to SCI will be denied until need-to-know is approved, eligibility determined, the SCI NDA is signed, and the SCI indoctrination is completed.

c. Any questions pertaining to SSBI submissions for SCI access should be addressed to the MARFORRES SSO at DSN 647-7238 or commercial (504)697-7238.

16. Personnel Security Management Network (PSMNET). The Personnel Security Management Network (PSMNET) on the JPAS must be established and maintained by the Site's Security Manager utilizing the Site's Security Management Office (SMO) Code. The PSMNET is established by uploading command personnel information listed on the Command's Alpha roster. Battalion level Commands can establish a PSMNet with multiple units only when they are co-located in the same site, otherwise each unit must establish and maintain their own PSMNet created under their SMO Code.

JAN 9 2015

Chapter 13

Information Technology (IT) Security Procedures

1. Basic Policy. IT security is the responsibility of every IT user in this headquarters. This responsibility includes the use and handling of all computers, telephonic, and video devices. DoN IT positions include any position in which the incumbent has access to DoN IT systems and/or performs IT-related duties with varying degrees of independence, privilege, and/or ability to access and/or impact sensitive data and information. Given the direct supporting relationship of DoN IT systems to the DoN national security mission, most DoN IT positions are sensitive.

2. IT Positions. In order to provide the appropriate level of background investigation and suitability adjudication, positions are designated according to potential risk. A sensitive position is any position whose occupant could bring about, by virtue of the nature of the position, an adverse effect on the national security.

a. IT Position Sensitivity Levels. The three sensitivity levels (and one none sensitive level) are listed below.

(1) Special-Sensitive (SS): Potential for inestimable impact and/or damage.

(2) Critical-Sensitive (CS): Potential for grave to exceptionally grave impact and/or damage.

(3) Noncritical Sensitive (NCS): Potential for some to serious impact and/or damage.

(4) Non-Sensitive (NS): Potential for no impact and/or damage as duties identified has limited relation to the mission.

b. IT Position Risk Levels. IT position risk levels are based on the level of automated privileges afforded, the level of fiscal privileges afforded, the scope of responsibilities, the level of independence and oversight afforded, and the ability to access sensitive information. The Office of Management and Budget (OMB) Circular A-130 provides the criteria for determining IT position risk levels. The national security

JAN 9 2015

mission is a primary consideration in all DoN IT position designations. The three basic DoN IT levels and one overarching DoN control levels are listed below.

(1) IT Designated Approving Authority (DAA): Exceptional Privilege; exceptional control

(2) IT-I: Privileged access

(3) IT-II: Limited Privilege, sensitive information access

(4) IT-III: No Privilege, no sensitive information access

3. Processing Classified Data on IT Equipment. The procedures for handling and processing classified information on IT equipment are generally the same as the procedures handling any other type of classified material. All disks, printer cartridges, hard copy documents, and any other products of classified information processing will be treated as classified material and handled in accordance with the procedures outlined in this document.

a. Before any automated system can be used to process classified data, the system must be accredited. Requests for authorization to process classified data shall be submitted to the IAM or Cyber Security Officer. Actions required during the accreditation process are detailed in the DoD Information Assurance Certification and Accreditation Process (DIACAP) (DoD I851.01).

b. Users shall possess the proper security clearance eligibility and access for the highest classification of data processed in the system and possesses the need to know for any of the information accessible through the system.

4. Software Security. All software will only be loaded by members of the G-6 IT support staff. Individuals will not load any personally procured software, and any attempts to circumvent security controls to load software will result in the individual user account and the network connection being immediately disabled.

5. System Security. Systems will be operated in "Systems High Mode." That is, only those individuals possessing the need-to-

JAN 9 2015

know and the requisite clearance access for the highest classification of data in the system (or any media accessible through the system), will be allowed access to the system.

a. Privately owned systems are not authorized to process classified information. In addition, privately owned software or public domain software from non-government sources are not authorized to process classified information. This security measure is designed to prevent a computer virus or other form of system contamination from occurring. Classified information will only be processed on U.S. Government equipment, in approved secure work spaces.

b. Environmental controls will be in accordance with the manufacturer's specifications. Sustained operation at the extremes of the manufacturer's suggested ranges may result in degraded equipment performance or failure.

6. IT Data Security. All media will be properly marked according to the highest classification of that data. Standard government labels (SF-710 for Unclassified, SF-707 for SECRET) will be used to the maximum extent possible. All IT equipment including computers, printers, copiers, scanners, and faxes will be labeled, and positioned and segregated from unclassified equipment with at least five feet of separation. It is the responsibility of the owning Command and/or Staff Section to order required marking materials.

a. Classified information must be properly controlled regardless of its form. Magnetic and optical media in any format (including hard drives, digital video disks (DVDs), and compact disks) will be included in semiannual classified material inventory or the change of custodian inventory. This inventory will be initiated by the Command and/or Staff Section Security Manager or assigned individual as part of the regular inspection process.

b. All controlled media storage devices, i.e. DVD, will be stored in a GSA approved container when not in use. Media devices will be afforded the full protection required for a classified document of the same classification.

7. Destroying Electronic Classified Data. Classified media will not be downgraded or declassified. Commands/Sections who have classified material for destruction will follow the guidelines for destruction in Chapter 9 of this Order.

JAN 9 2015

8. Transmission Equipment. No transmission equipment (i.e., STE, modems, LAN cables, etc.) will be connected to equipment used to process classified data unless approved in writing by the MARFORRES G-6 IAM or Cyber Security Officer. A request to connect such equipment will be submitted to the IAM or Cyber Security Officer via the MARFORRES G-6 Share Portal or the G-6 Service Desk. This request will contain the nomenclature of the equipment to be connected and the justification. Upon receipt of the request, the G-6 ADPSO will evaluate the request based on the equipment to be used and justification and endorse the request with comments.

9. Spillages. A spillage occurs when information of a higher classification is used on a system of a lower classification (i.e. SECRET information used on the NIPRNET). In no case will, Deputy Command Security Manager classified information be transmitted over an unclassified network.

a. If information is accidentally transferred, or if classified or suspected classified information is received over an unclassified network it will not be forwarded, and the MARFORRES Command Security Manager and the MARFORRES Information Assurance Officer Manager or Cyber Security Officer will be notified immediately.

b. When notified of a potential spillage, the Command Security Manager, Deputy Command Security Manager and the Information Assurance Officer Manager or Cyber Security Officer will assist the recipient with completing required reporting information, notifying the Marine Corps Network Operations and Security Center (MCNOSC). The Command Security Manager, Deputy Command Security Manager and the Information Assurance Officer Manager or Cyber Security Officer will maintain oversight of the spillage investigation and ensure regular testing and training for Cyber Security and Security Awareness is conducted.

10. Network Access. Access to the network (RNET) will be authorized only after verifying a user's clearance eligibility and need-to-know. A Systems Authorization Access Request (SAAR) Form DD-2875 will be utilized for this purpose, and routed via the MARFORRES G6 Share Portal.

a. Additionally, the supervisor will verify that the individual has completed Information Assurance and Cyber Security refresher training within the past year. The certificates of completion are required in the SAAR routing and

JAN 9 2015

approval process. Users that do not maintain current training will be lose access eligibility. Users that do not access their accounts for an extended period of time may lose access eligibility, and will need to resubmit a SAAR for approval.

11. Wireless Devices and PED. Wireless devices present an inherent vulnerability and are prohibited in classified spaces by the Defense Information Systems Agency (DISA).

a. Wireless devices or PED (i.e. cell phones, iPads, iPods, or Blackberries) will not be permitted in classified areas at any time, and will be stored outside the space in the designated lockers. Air cards will not be inserted into unclassified laptops in classified areas unless authorized by the Command Security Manager or the COMMARFORRES.

b. Commands and/or Staff Sections will perform regular inspections of classified work areas for violations.

JAN 9 2015

APPENDIX A

REFERENCES

Executive Order 12958, as Amended, Classified National Security Information, 25 Mar 03

DoD Directive 5200.1-R, DoD Information Security Program

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), Feb 05

DoD 5200.33-R, Defense Courier Service, 24 Jun 02

DoD 8500.1, Information Assurance, October 24, 2002

DoD I5200.08, Security of DoD Installations and Resources, December 10, 2005

SECNAV M-5510.30A, Department of the Navy Personnel Security Program Regulation

SECNAV M-5510.36, Department of the Navy Information Security Program Regulation

SECNAV M-5210.1, Records Management Manual, Dec 05

EKMS-1, Communications Material Security Policy and Procedures for Navy Electronic Key Management System

NWP 1-01A, Naval Warfare Publication System

SECNAVINST 5720.42F, DoN Freedom of Information Act (FOIA) Program, 6 Jan 99

OPNAVINST 5513.1F, Department of the Navy Security Classification Guidance

OPNAVINST C5510.101D, NATO Security Procedures

OPNAVINST 5530.14B, Physical Security and Loss Prevention

MCO 5239.2, Marine Corps Information Assurance (IA) Program

IRM 5239-13, System Security Plan

ForO 5510.1A

JAN 9 2015

MCO P5510.18A, Marine Corps Information and Personnel Security
Program Manual

MCO P5530.14, Marine Corps Physical Security Program Manual

JAN 9 2015

APPENDIX B

ACRONYMS

02XX - Intelligence MOS
26XX - Intelligence MOS
ACS - Access Control System
ANACI - Access National Agency Check with Inquiries
ATFP - Anti-Terrorism Force Protection
ATTO - Anti-Terrorism Training Officer
C4 - Command Control, Communications, Computers
CAA - Controlled Access Areas
CAC - Common Access Card
CAF - Central Adjudication Facility
CBRN - Chemical Biological Radiation and Nuclear
CCTV - Closed Circuit Television
CG - Commanding General
CIK - Crypto Ignition Key
CLNC - Clearance
CMS - Communication Security Management
CO - Commanding Officer
COMMARFORRES - Commander, Marine Forces Reserve
COMSEC - Communication Security Equipment
CRYPTO - Cryptographic
CS - Critical Sensitive
CUI - Controlled Unclassified Information
DCID - Director Central Intelligence Directive
DCS - Defense Carrier Service
DIACAP - DoD Information Assurance Certification and Accreditation Process
DISA - Defense Information Systems Agency
DOD - Department of Defense
DON - Department of Navy
DVD - Digital Video Disks
EAP - Emergency Action Plan
EKMS COI - Electronic Key Management System Course of Instruction
EDIPI - Electronic Data Interchange Personal Identifier
ENTNAC - Entrance National Agency Check
EQIP - Electronic Questionnaires Investigation Processing
ESS - Electronic Security Systems
FA - Functional Area
FSO - Facility Security Officer
GS - General Schedule
GSA - General Service Administration
HCI - Highest Classification Indicator

JAN 9 2015

APPENDIX B

ACRONYMS

02XX - Intelligence MOS
26XX - Intelligence MOS
ACS - Access Control System
ANACI - Access National Agency Check with Inquiries
ATFP - Anti-Terrorism Force Protection
ATTO - Anti-Terrorism Training Officer
C4 - Command Control, Communications, Computers
CAA - Controlled Access Areas
CAC - Common Access Card
CAF - Central Adjudication Facility
CBRN - Chemical Biological Radiation and Nuclear
CCTV - Closed Circuit Television
CG - Commanding General
CIK - Crypto Ignition Key
CLNC - Clearance
CMS - Communication Security Management
CO - Commanding Officer
COMMARFORRES - Commander, Marine Forces Reserve
COMSEC - Communication Security Equipment
CRYPTO - Cryptographic
CS - Critical Sensitive
CUI - Controlled Unclassified Information
DCID - Director Central Intelligence Directive
DCS - Defense Carrier Service
DIACAP - DoD Information Assurance Certification and Accreditation Process
DISA - Defense Information Systems Agency
DOD - Department of Defense
DON - Department of Navy
DVD - Digital Video Disks
EAP - Emergency Action Plan
EKMS COI - Electronic Key Management System Course of Instruction
EDIPI - Electronic Data Interchange Personal Identifier
ENTNAC - Entrance National Agency Check
EQIP - Electronic Questionnaires Investigation Processing
ESS - Electronic Security Systems
FA - Functional Area
FSO - Facility Security Officer
GS - General Schedule
GSA - General Service Administration
HCI - Highest Classification Indicator

JAN 9 2015

SES - Senior Executive Service
SF - Standard Form
SI - Special Intelligence
SIPRNET - Secret Internet Protocol Router Network
SKL - Simple Key Loader
SMO - Security Management Office
SOP - Standard Operating Procedures
SS - Special Sensitive
SSA - Security Servicing Agreement
SSBI - Single Scope Background Investigation
SSO - Special Security Officer
STU III - Secure Telephone Unit Third Generation
T/O - Table of Organization
TEMP - Temporary
TS - Top Secret
TSCA - Top Secret Control Assistant
TSCO - Top Secret Control Officer
UA - Unauthorized Absence
USI - Unannounced Security Inspections
USMC - United States Marine Corps
USPS - United States Postal Service
VIP - Very Important Person
XO9 - High Security Electromechanical Lock