



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

MCO 5510.18B
PPO
30 JAN 2017

MARINE CORPS ORDER 5510.18B

From: Commandant of the Marine Corps
To: Distribution List

Subj: UNITED STATES MARINE CORPS INFORMATION AND PERSONNEL
SECURITY PROGRAM (IPSP)

Ref: See enclosure (1)

Report Required: Agency Information Security Program Data
Report (Report Control Symbol 5510-22
(External RCS DD-INT(AR)1418)),
Chap. 2, par. 13b

Encl: (1) References
(2) Marine Corps IPSP Procedural Guidance

1. Situation. This Order establishes the Marine Corps Information and Personnel Security Program (IPSP) under the authority of references (a) through (g) and in compliance with references (h) through (ad).

2. Cancellation. MCO P5510.18A and MCO 5510.17.

3. Mission. All commands and organizations within the Marine Corps shall ensure compliance and implement the provisions of this Order to protect classified information and ensure personnel are properly vetted to handle such information.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent

(a) Purpose. Apply uniform, consistent, and cost-effective policies and procedures for the classification, safeguarding, transmission, and destruction of classified

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

30 JAN 2017

National Security Information (NSI); authorize initial and continued access to classified information and/or initial and continued assignment to sensitive duties to those persons whose loyalty, reliability and trustworthiness are such that entrusting them with classified information or assigning them to sensitive duties is clearly consistent with the interests of national security.

(b) End State. Commanding Officers implement IPSP(s) and Sensitive Compartmented Information (SCI) security program(s) within internal and external elements.

(2) Concept of Operations

(a) Pursuant to authorities and responsibilities outlined in references (a) through (g), Headquarters Marine Corps (HQMC), Plans, Policies and Operations Department (PP&O), Security Division (PS), shall administer the IPSP for the Marine Corps.

(b) HQMC PS shall conduct annual reviews/inspections of security programs at Marine Corps installations and commands as a member of the Inspector General of the Marine Corps (IGMC) inspection team or independently, as required. Independent inspections are typically conducted annually on all Marine Forces (MARFOR) level commands and other organizations as circumstances may allow.

(c) Pursuant to authorities and responsibilities outlined in references (a), (g), and (j), the Director of Intelligence (DIRINT) shall administer and manage the SCI security program for the Marine Corps to include providing instructions, training programs, and procedures to investigate security violations, compromises, and unauthorized disclosures related to SCI information.

(d) DIRINT, through the HQMC Special Security Office (SSO), shall conduct annual reviews and/or inspections of SCI security programs at Marine Corps installations and commands.

b. Tasks

(1) Commanding Officers shall:

(a) Implement IPSP(s) and SCI security program(s) within internal and external elements.

30 JAN 2017

(b) Ensure all Marines are screened upon arrival at their commands, whether training or operational, to ensure the Commanding Officer is fully aware of the Marine's Personnel Security Investigation (PSI) status and any potential derogatory issues.

(c) Consider administrative, non-judicial and judicial remedies for all compromises of classified NSI and other significant security violations.

(2) Commanding General, Marine Corps Recruiting Command (CG MCRC) shall:

(a) Ensure the required PSI, identified in Chapter 5 of this Order, is properly prepared, submitted to the Office of Personnel Management (OPM), and monitored prior to shipping recruits to recruit training.

(b) Review the status of the PSI and eligibility determination at least 24 hours prior to shipping. Those with no eligibility determination shall be identified to the appropriate recruit depot security manager for further monitoring, as appropriate.

(3) Commanding General, Training and Education Command (CG TECOM) shall ensure the required PSIs, identified in Chapter 5 of this Order, are submitted and received by the OPM prior to the Marine departing recruit training or The Basic School (TBS).

(a) TECOM will ensure that all Marines have an open investigation, populated in the Joint Personnel Adjudication System (JPAS), prior to departing the TECOM educational and training pipeline.

(b) HQMC SSO and Marine Corps Recruit Depot (MCRD) screening representatives will execute SCI pre-screening and eligibility interviews for Marine officers at TBS, billet re-assignments, and enlisted Marines on behalf of the Commanding Officer TBS and Commanding Generals of the recruit depots.

c. Coordinating Instructions

(1) The term Commanding Officer is used throughout this Order as a generic term for the head of an organizational entity (e.g., Commander, Commanding General, Officer-in-Charge, Director, etc.) whose duties include:

30 JAN 2017

(a) Authorizing the submission of requests for investigation.

(b) Assigning access to classified material.

(c) Assigning Temporary Access (formerly interim access) pending the completion of standard PSI.

(2) The 2012 Federal Investigative Standards (FIS) established requirements for conducting background investigations to determine eligibility for logical and physical access, suitability for U.S. Government employment, fitness to perform work for, or on behalf of, the U.S. Government as a contract employee, and eligibility for access to classified information or to hold a sensitive position. The standards consist of five tiers with phased implementation.

(a) References (r) and (s) announce tier designations and include a phased implementation schedule. Due to the anticipated time to transition to new standards and increased familiarity with tier naming conventions, PSI will be depicted throughout this Order in the following format:

1. National Agency Check and Inquiries (NACI)/Tier 1 (T1). T1 in lieu of the former NACI.

2. National Agency Checks with Law and Credit (NACLC)/Tier 3 (T3)/Tier 3 Reinvestigation (T3R). T3/T3R in lieu of the former NACLC.

3. Access National Agency Checks with Inquiries (ANACI)/T3/T3R. T3 and T3R in lieu of the former ANACI.

4. Single Scope Background Investigation (SSBI)/Tier 5 (T5). T5 in lieu of the former SSBI.

5. SSBI-PR/T5R. T5R in lieu of the former SSBI-Periodic Reinvestigation.

(b) Tier 2 and Tier 4 investigations are required for positions of public trust, but which do not require access to sensitive or national security information. Tier 2 and Tier 4 investigations are not applicable to the Marine Corps IPSP.

(3) Responsibilities assigned to the Commanding Officer by this Order may be delegated unless specifically prohibited.

30 JAN 2017

(4) This Order is to be the primary source to ensure standardization of the IPSP. If conflicts arise between the varied Department of Defense (DoD) and Department of the Navy (DON) information and personnel security references, the DoD information and personnel security references provide the final guidance.

(5) Policy and procedural or "how to" guidance is contained in enclosure (2).

(6) This Order applies to all personnel (e.g., Marines, Navy personnel assigned/attached to a Marine Corps command, government civilian employees, contractors, and consultants) employed by, and/or working in any element of the Marine Corps.

5. Administration and Logistics

a. Recommendations concerning the content of this Order may be forwarded to PS via the appropriate chain-of-command.

b. All related collateral reports, recommendations, and waiver and exception requests shall be submitted to the Deputy Under Secretary of the Navy for Policy (DUSN (P)), via HQMC PS, per the provisions of references (t) and (u), unless otherwise indicated.

c. All related SCI security program reports, recommendations, and waiver requests shall be submitted to Special Security Office of the Navy (SSO Navy), via HQMC SSO, per the provisions of reference (j).

d. Privacy Act. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. The DON recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected. The DON's need to collect, use, maintain, or disseminate PII about individuals for purposes of discharging its statutory responsibilities will be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII will be in accordance with the Privacy Act of 1974, as amended (reference (v)) and implemented per reference (ad).

e. Records created as a result of this Order shall be managed according to National Archives and Records Administration approved dispositions per references (x) to

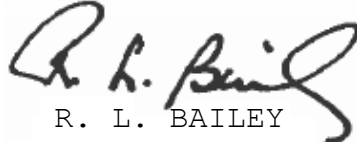
30 JAN 2017

ensure proper maintenance, use, accessibility and preservation, regardless of format or medium.

6. Command and Signal

a. Command. This Order is applicable to the Marine Corps Total Force.

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

A handwritten signature in black ink, appearing to read "R. L. Bailey". The signature is stylized and cursive.

R. L. BAILEY
Deputy Commandant for
Plans, Policies, and Operations

DISTRIBUTION: PCN 10208490600

- Ref:
- (a) MCO 5311.6
 - (b) Executive Order 12968, Access to Classified Information, August 04, 1995
 - (c) Executive Order 13526, Classified National Security Information, December 29, 2009
 - (d) Executive Order 10450, Security Requirements for Government Employees, April 27, 1953
 - (e) Executive Order 12829, National Industrial Security Program, January 08, 1993
 - (f) Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008
 - (g) Executive Order 12333, United States Intelligence Activities, as amended July 30, 2008
 - (h) DoD 5220.22-M, National Industrial Security Program Operating Manual, Change 2, May 18, 2016
 - (i) DoD 5220.22-R, Industrial Security Regulation, December 1985
 - (j) DoD Manual 5105.21, Volume 3, Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities, October 19, 2012
 - (k) DoD Manual 5200.01, Vol 1-IV, DoD Information Security Program, February 24, 2012, Incorporating Change 2, March 19, 2013
 - (l) DoD Instruction 5200.02, DoD Personnel Security Program (PSP), Incorporating Change 1, Effective September 09, 2014
 - (m) DoD Instruction 3305.13, DoD Security Education, Training, and Certification, February 13, 2014
 - (n) DoD Instruction 1000.30, Reduction of Social Security Number (SSN) Use Within DoD, August 1, 2012
 - (o) DoD Directive 5100.55, United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN), February 27, 2006
 - (p) Intelligence Community Policy Guidance (ICPG) 704.4, Reciprocity of Personnel Security Clearance and Access Determinations, October 02, 2008
 - (q) Homeland Security Presidential Directive-12, Policies for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
 - (r) Federal Investigations Notice 15-03, Implementation of Federal Investigative Standards for Tier 1 and Tier 2 Investigations, November 04, 2014
 - (s) Federal Investigations Notice 16-02, Federal

30 JAN 2017

Investigative Standards for Tier 3 and Tier 3
Reinvestigation, October 06, 2015

- (t) SECNAV M-5510.36
- (u) SECNAV M-5510.30
- (v) SECNAVINST 5211.5E
- (w) SECNAV M-5210.2
- (x) SECNAV M-5210.1
- (y) MCWP 3-40.1 w/chg 1
- (z) MCO 5530.14A
- (aa) MCO 5600.31A
- (ab) MCO 5430.1
- (ac) MCO 5239.2B
- (ad) 5 U.S.C. 552a

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporated Change

TABLE OF CONTENTS

<u>IDENTIFICATION</u>	<u>TITLE</u>	<u>PAGE</u>
Chapter 1	INTRODUCTION.....	1-1
1.	Purpose.....	1-1
2.	Applicability.....	1-1
3.	Scope.....	1-1
4.	Assistance Via the Chain of Command.....	1-2
5.	Combat Operations.....	1-3
6.	Waivers and Exceptions.....	1-4
7.	Alternative Compensatory Control Measures.... (ACCM)	1-4
8.	Position Sensitivity Designation (PSD).....	1-4
9.	Use of Social Security Numbers (SSN).....	1-6
10.	Command Echelon.....	1-6
Chapter 2	COMMAND SECURITY MANAGEMENT.....	2-1
1.	Basic Policy.....	2-1
2.	Commanding Officer Responsibilities.....	2-1
3.	Command Security Manager.....	2-2
4.	Duties of the Command Security Manager.....	2-4
5.	Top Secret Control Officer (TSCO).....	2-6
6.	Security Assistants.....	2-6
7.	Contracting Officer's Security Representative (COSR)	2-7
8.	Information System Security Manager (ISSM)...	2-8
9.	Special Security Officer (SSO).....	2-8
10.	Inspections, Assist Visits and Reviews.....	2-9
11.	Security Servicing Agreements (SSA).....	2-11
12.	Planning for Emergencies.....	2-12
13.	Annual Reporting Requirements.....	2-12
Chapter 3	SECURITY EDUCATION.....	3-1
1.	Basic Policy.....	3-1
2.	Responsibilities.....	3-1
3.	Minimum Requirements.....	3-2
4.	Training for Security Personnel.....	3-3
5.	Resources.....	3-5
Chapter 4	INFORMATION SECURITY.....	4-1
1.	Basic Policy.....	4-1
2.	Classification Management.....	4-2

30 JAN 2017

3.	Applicability of Control Measures.....	4-2
4.	Top Secret Control Measures.....	4-3
5.	Secret and Confidential Control Measures.....	4-3
6.	Classified Hard Disk Drives (HDD).....	4-5
7.	Working Papers.....	4-5
8.	Controlled Unclassified Information (CUI)....	4-6
9.	Reproduction.....	4-6
10.	Classified Electronically Transmitted Information.....	4-8
11.	Classified Documents on External Media.....	4-9
12.	Security Violations.....	4-9
13.	Practices Dangerous to Security.....	4-11
14.	Destruction of Classified Material.....	4-11
15.	Foreign Disclosure.....	4-11

Chapter 5 PERSONNEL SECURITY.....5-1

1.	Basic Policy.....	5-1
2.	Access.....	5-6
3.	Local Records Checks.....	5-8
4.	Temporary Access.....	5-9
5.	Types of Personnel Security Investigations...	5-10
6.	Adjudicative Entries.....	5-13
7.	Continuous Evaluation Program (CEP).....	5-15
8.	Pre-Screening.....	5-18
9.	Adverse Actions.....	5-20
10.	Joint Personnel Adjudication System (JPAS)...	5-23
11.	Electronic Questionnaire for Investigations..	5-26
	Processing (e-QIP)	

Chapter 6 INDUSTRIAL SECURITY.....6-1

1.	Basic Policy.....	6-1
2.	Contracting Officer's Security Representative. (COSR)	6-1
3.	Contractor Access to Classified NSI.....	6-2
4.	Contracting Officer's Representative Training.	6-2
5.	Security Training for Contractors.....	6-3
6.	Continuous Evaluation for Contractors.....	6-3

Chapter 7 NORTH ATLANTIC TREATY ORGANIZATION (NATO)....7-1

1.	Basic Policy.....	7-1
2.	Responsibilities.....	7-1
3.	NATO Control Point.....	7-1
4.	User Offices.....	7-2

30 JAN 2017

5.	NATO Information.....	7-3
6.	Access and Investigative Requirements.....	7-3
7.	Briefing/Re-briefing/Debriefing.....	7-3
8.	Control and Handling.....	7-5
9.	Storage.....	7-5
10.	Reproduction and Extracts.....	7-5
11.	Transportation and Transmission.....	7-5
12.	NATO on SIPRNET.....	7-6
13.	Electronic Mail.....	7-6
14.	Destruction.....	7-6
15.	Compromise.....	7-7
16.	Espionage, Sabotage, Terrorism, and Deliberate Compromise.....	7-7
APPENDIX A	GLOSSARY.....	A-1
APPENDIX B	DEFINITIONS.....	B-1
APPENDIX C	GUIDELINES FOR COMMAND SECURITY INSTRUCTION/TURNOVER BINDER.....	C-1
APPENDIX D	EMERGENCY PLAN AND EMERGENCY DESTRUCTION SUPPLEMENT.....	D-1
APPENDIX E	COMMANDER'S CHECKLIST FOR GRANTING ACCESS....	E-1
APPENDIX F	TEMPORARY ACCESS AUTHORIZATION LETTER FORMAT.....	F-1
APPENDIX G	CLASSIFIED MATERIAL CONTROL CENTER.....	G-1
APPENDIX H	COLLATERAL SECURITY INCIDENT FLOWCHART.....	H-1
APPENDIX I	PRIVACY ACT STATEMENT.....	I-1

Chapter 1

Introduction

1. Purpose. The Marine Corps IPSP is established to implement standards and procedures as required by references (a) through (ad) to:

a. Apply uniform, consistent, and cost-effective policies and procedures for the classification, safeguarding, transmission, and destruction of classified NSI.

b. Authorize initial and continued access to classified information and/or initial and continued assignment to sensitive duties to those persons whose loyalty, reliability and trustworthiness are such that entrusting them with classified NSI or assigning them to sensitive duties is clearly consistent with the interests of national security.

2. Applicability. This Order applies to all personnel (e.g., Marines, Navy personnel assigned/attached to a Marine Corps command, government civilian employees, contractors and consultants) employed by, and/or working in any element of the Marine Corps.

a. Contracting Officers shall ensure compliance with applicable policy by properly coordinating with Command Security Managers, Contracting Officer Security Representatives (COSR), and the Defense Security Service (DSS) prior to completion of contract negotiations in which provisions for access to classified NSI is required.

b. References (e), (f), and Chapter 6 of this Order provide specific information concerning contractors working with classified NSI.

3. Scope. This Order establishes the minimum standards for the Marine Corps IPSP.

a. Commanding Officers are responsible for compliance with this Order.

b. This Order provides guidance on command security management, security education, information security, personnel security, industrial security, and NATO information security.

30 JAN 2017

c. The term classified NSI is generically used throughout this Order to identify any matter, document, product, substance, or item of equipment, on or in which classified NSI is recorded or embedded.

4. Assistance Via the Chain of Command

a. Marine Corps activities are required to obtain collateral related guidance or interpretation of policy and procedures in this Order from PS via the operational chain of command.

(1) Telephone inquiries may be made to HQMC PS (703.695.7162).

(2) Current contact information is available on the HQMC PS, IPSP SharePoint website:
<https://ehqmc.usmc.mil/org/hqmcppo/PS/PSS/Blog/Shared%20Documents/Forms/AllItems.aspx>

(3) After-hours voice-mail is available (703.695.7162).

(4) The Marine Corps IPSP organizational email address is ipsp_admin@usmc.mil.

(5) Attempts to contact HQMC PS should only be used after attempts to resolve issues via the chain of command have been exhausted.

(6) Marine Corps commands shall not contact DUSN(P) directly.

b. Marine Corps activities are required to obtain SCI security program related guidance or interpretation of policy and procedures in this Order from HQMC SSO via the operational chain of command.

(1) Telephone inquiries may be made to HQMC SSO (703.693.6005).

(2) HQMC SSO organizational email address is hqmc_intel_sso@usmc.mil.

(3) Attempts to contact HQMC SSO should only be used after attempts to resolve issues via the chain of command have been exhausted.

30 JAN 2017

5. Combat Operations. Recognizing that combat can create special circumstances, conditions may dictate a modification to these guidelines. Commanding Officers may modify the requirements of this Order as necessary to meet local conditions during combat, combat-related, or contingency operations. This provision does not apply to training exercises, including those preparatory to combat deployment.

a. Access granted to classified NSI based on this paragraph must be a command-level decision based on a risk assessment of the information to be accessed, and the person to whom access is granted.

(1) This paragraph is not to be used as a means to circumvent the standard personnel security process available during the pre-deployment period.

(2) Deviations are only authorized as a matter of life threatening or operational necessity.

b. The individual shall complete the **CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT STANDARD FORM 312 (Rev.7-2013)** and receive a security orientation brief if collateral access is granted based on this exception. The individual shall complete the **SENSITIVE COMPARTMENTED INFORMATION NON DISCLOSURE AGREEMENT FORM 4414** and receive SCI orientation brief by SSO personnel if SCI access is granted.

(1) Notification (e.g., encrypted email, secure FAX, SIPR email, etc.) shall be made to HQMC PS or HQMC SSO at the first available opportunity.

(2) This notification shall include the:

(a) Full name.

(b) Social Security Number(SSN)/DoD ID Number.

(c) Individual's date of birth.

(d) Description of the nature and type of information to which the individual was granted access.

(e) Duration of time the individual will have access to this information.

30 JAN 2017

(f) Justification for the intentional deviation from policy.

c. This paragraph does not allow access to individuals who have been adjudicated by the DoD Consolidated Adjudications Facility, Navy Division (DODCAF DON), as being ineligible for access, as these decisions represent the determination that the individual is an unacceptable security risk.

d. Modifications to storage requirements in a field environment must pay particular attention to the threat to ensure that classified NSI is not placed at risk.

6. Waivers and Exceptions. Waivers and exceptions relating to physical security within this Order must be requested from the Deputy Commandant (DC), PP&O.

7. Alternative Compensatory Control Measures (ACCM). Commanding Officers desiring to implement ACCM must submit requests to DUSN(P), via HQMC PS. Procedures for submitting requests and requirements for approval are outlined in reference (t).

8. Position Sensitivity Designation (PSD). Military positions are, by default, considered to be sensitive. This designation is supported by the investigative requirement of a NACLIC/T3 for enlistment/appointment suitability.

a. The favorable adjudication of the NACLIC/T3, with the assignment of secret eligibility, does not automatically grant access to classified NSI. However, it does make the individual eligible for information technology (IT) Level II privileges.

(1) A favorable determination suggests a level of reliability and trustworthiness commensurate with access to sensitive information or assignment to a sensitive position.

(2) If a military member is not eligible for access to classified NSI, the individual's commander may not assign the individual to sensitive duties or allow access to sensitive information and sensitive IT systems.

b. Government civilian positions require a determination at the time of Position Description (PD) creation or revision concerning PSD. The sensitivity level assigned to the PD shall determine which investigation is authorized for submission for the individual. PSD(s) must be made in consultation with local

Human Resource (HR) offices, the employing office, and the Command Security Manager.

c. Many civilian positions are sensitive at some level and shall require an investigation that will result in the assignment of clearance eligibility whether or not access to classified NSI is required. Reference (u) outlines the investigative requirement for each PSD.

(1) Those positions designated "non-sensitive" (no classified and no sensitive information access) require the NACI/T1. The **Questionnaire for Non-Sensitive Positions Standard Form 85 Revised December 2013** is used to conduct these investigations.

(2) Those positions requiring access to Secret or sensitive information or IT II computer privileges require the ANACI/T3/T3R). The **Questionnaire for National Security Positions Standard Form 86 Revised December 2010** is used to conduct these investigations.

(3) Those positions which require access to Top Secret information, designated critical-sensitive, special-sensitive, and/or IT Level I, require the SSBI/T5.

(a) The **Questionnaire for National Security Positions Standard Form 86 Revised December 2010** is used to conduct these investigations.

(b) The Billet Identification Code (BIC) must be coded with a "T".

d. Marine Corps Systems Command (MCSC) is the acquisition command for the Marine Corps and is a Competency Aligned Organization (CAO).

(1) BICs, billets, and personnel may be moved from one program to another to support acquisition strategies throughout a program's life cycle.

(2) MCSC shall track their "T" coded BIC structure in their locally maintained Competency Management Tool (CMT).

9. Use of SSN. Use of the full SSN will be consistent with the requirements of reference (n) and avoided wherever possible.

30 JAN 2017

a. However, if use of the SSN becomes necessary, utmost care must be exercised in handling this information due to the sensitivity of the SSN.

b. If the individual does not possess documentation containing his/her DoD ID Number or SSN, either may be provided verbally or in writing, in a manner designed to prevent access by others. When using this method, data contained on the provided documentation must match PII on the Person Summary Screen in JPAS.

(1) If requesting PII for identification purposes only (and not entering the information into a system or form) a Privacy Act Advisory (PAA) must be provided.

(2) A PAA is similar to a Privacy Act Statement (PAS). It provides the authority and purpose for requesting the SSN and whether providing the SSN is voluntary or mandatory.

c. Use of the SSN is guided by the Privacy Act of 1974, as amended, and reference (n). Each request for an individual's SSN must be accompanied by a copy of the PAS.

(1) Appendix J includes a PAS for use when collecting data for the purpose of granting/denying classified data access.

(2) The PAS must be made available to anyone from whom the SSN is solicited.

(3) Use of the SSN on any access roster or document posted and viewable by the general population of an organization is strictly prohibited.

(4) Rosters should never contains SSNs.

(5) Posting the SSN where anyone without a Need-to-Know can view it is prohibited (not just exterior).

(6) Rosters containing a list of personnel should only be posted where all potential viewres have a definable Need-to-Know (i.e., not in common passage ways or on exterior doors). See also MCO 5530.14A (Access Rosters).

(7) Further, use of SSNs in entry and exit logs is also prohibited as it exposes the SSN to individuals without an established, official requirement for access to the SSN.

30 JAN 2017

10. Command Echelon

a. The Marine Corps does not typically use the term, "echelon of command" when describing degree of authority for program responsibility. However, references (t) and (u) use this descriptive term to delegate various authorities within this program and therefore additional guidance is warranted in this Order.

b. For clarification purposes, HQMC is the only "Echelon 1" command within the Marine Corps. All MARFOR level commands and separate commands which report directly to HQMC are considered to be "Echelon 2" commands with all the authorities established in the references. All organizations shall follow the chain of command.

Chapter 2

Command Security Management

1. Basic Policy. Commanding Officers are responsible for compliance with and implementation of the Marine Corps IPSP or applicable SCI security program within their command. The effectiveness of the command's IPSP and SCI security program depends on the importance given by the Commanding Officer.

2. Commanding Officer Responsibilities. An effective IPSP relies on a team of professionals working together to fulfill the Commanding Officer's responsibilities.

a. Command security management responsibilities include:

(1) Designate a Command Security Manager in writing.

(2) Designate a Top Secret Control Officer (TSCO) in writing if the command handles Top Secret information.

(3) Designate an Information System Security Manager (ISSM) in writing if the command processes data in an automated system.

(4) Designate a Security Officer in writing to manage facilities security.

(5) Designate a SSO in writing to administer the command SCI security program.

(6) Issue a written command security instruction. See Appendix C.

(7) Establish and maintain a self-inspection program. The self-inspection program must include security inspections, program reviews, and assist visits to evaluate and assess the effectiveness of the command and its subordinate command's IPSP. Reference (t) provides detailed instruction.

(8) Establish an industrial security program when the command engages in classified procurement or when cleared contractors operate within the areas under the Commanding Officer's control.

(9) Ensure that the Command Security Manager and other command security professionals are appropriately trained, that

30 JAN 2017

all personnel receive required security education and that the command has a robust security awareness program.

(10) Prepare an Emergency Action Plan (EAP) for the protection of classified material.

(11) Ensure the command security inspections, program reviews, and assist visits are conducted for effectiveness of the IPSP in subordinate commands.

(12) Ensure that the performance rating systems of all Marine Corps military and civilian personnel whose duties significantly involve the creation, handling, or management of classified NSI include a security element on which to be evaluated.

(13) Ensure implementation and required use of JPAS.

(14) Ensure implementation of the DoD Continuous Evaluation Program (CEP).

b. Consideration must be given to continuation of program management responsibilities during deployments for operations and exercises.

(1) Billets occupied by civilian employees must be reviewed in relation to PD(s) and deployment requirements.

(2) Remain Behind Elements (RBE) must have an individual designated as the Command Security Manager and, as appropriate, ensure that a Security Servicing Agreement (SSA) has been created for security services.

3. Command Security Manager. Commands in the Marine Corps eligible to receive classified NSI (e.g., all Squadron/Battalion level commands and above), are required to designate, in writing, a Command Security Manager per references (k) and (t).

a. All Command Security Manager appointment letters shall be uploaded to the HQMC PS site at <https://ehqmc.usmc.mil/org/hqmcppo/PS/PSS/Blog/default.aspx>. Click on the link, "Security Manager Appointment Letters" and the click on "Add a Document."

b. On occasion, separate commands below the Squadron/Battalion level may also require a Command Security

30 JAN 2017

Manager depending on the mission and support available from parent commands.

c. A unit's choice to divest itself of current classified holdings is not sufficient to negate this requirement.

d. Due to the technical nature of the IPSP and applicable SCI security program, and the intricacies involved with program management for the programs, the Command Security Manager and SSO should be assigned as a primary, full-time duty at every available opportunity.

e. The Command Security Manager shall be a special staff officer and afforded direct access to the Commanding Officer to ensure effective management of the command's IPSP. Reference (y) requires the Command Security Manager and SSO to report directly to the Chief of Staff (CoS) or Executive Officer (XO).

f. The presence of a Command Security Manager goes well beyond the management of classified NSI/material. They administer the Personnel Security Program, the Insider Threat Program, and manage Controlled Unclassified Information (CUI). The Command Security Manager supports PII protection when applied to other command applications (e.g., Human Resources (HR), Comptroller, Law Enforcement (LE)).

g. The Command Security Manager must be a military officer or civilian employee in the grade of GS-11 or above, with sufficient authority and staff to manage the IPSP for the command.

h. The Command Security Manager must be a U.S. citizen and have been the subject of a favorably adjudicated SSBI/T5 completed within the five years prior to assignment.

i. Though typically assigned as a collateral duty to XOs in operational commands, this duty may be assigned to any other officer in the command provided he or she can devote the necessary time and effort to effectively comply with all program requirements.

j. Commanding Officers shall allow for the formal training of security managers and assistant security managers within 180 days of appointment. Training requirements are described in Chapter 3 of this Order.

30 JAN 2017

k. Each command shall prepare and maintain a written command security instruction, specifying how security procedures and requirements shall be accomplished in the command. Appendix C applies.

4. Duties of the Command Security Manager

a. The duties of the Command Security Manager are delineated in references (k) and (t). The Command Security Manager is the principal advisor to the Commanding Officer on the IPSP and is responsible to the Commanding Officer for the management of the program.

(1) The duties described in this Order may apply to a number of personnel.

(2) The Command Security Manager must be cognizant of command security functions and the command's mission to ensure the security program is coordinated and inclusive of all requirements.

(3) The Command Security Manager must ensure that those in the command who have security duties are kept abreast of changes in policies and procedures, and must provide assistance in solving security problems.

(4) The Command Security Manager plays a critical role in developing and administering the command's IPSP.

b. The duties listed below apply to all Command Security Managers:

(1) Serves as the Commanding Officer 's advisor and direct representative in matters pertaining to the classification, safeguarding, transmission and destruction of classified NSI and CUI.

(2) Serves as the Commanding Officer's advisor and direct representative in matters regarding the eligibility of personnel to access classified NSI and assignment to sensitive duties.

(3) Develops written command IPSP procedures, including an EAP which integrates emergency destruction plans, where required.

30 JAN 2017

(4) Develops an annually updated turnover binder to ensure continuity of the command's security program. Refer to Appendix C.

(5) Formulates and coordinates the command's security awareness and education program.

(6) Ensures security control of visits to and from the command when the visitor requires, and is authorized, access to classified NSI.

(7) Ensures that all personnel who shall handle classified NSI or shall be assigned to sensitive duties are appropriately cleared through coordination with the DODCAF DON and that requests for personnel security investigations are properly prepared, submitted and monitored.

(8) Ensures that access to classified NSI is limited to those who are eligible and have a verifiable Need-to-Know.

(9) Ensures that PSI, eligibility, and accesses are properly recorded within JPAS.

(10) Coordinates the command Continuous Evaluation Program (CEP).

(11) Maintains liaison with the command SSO concerning information and personnel security policies and procedures.

(12) Coordinates with the command ISSM on matters of common concern.

(13) Coordinates with the local Naval Criminal Investigative Service (NCIS) field office to ensure a steady flow of information related to the Marine Corps Insider Threat Program (MCInTP) and the CEP.

(14) Ensures that all personnel who have had access to classified NSI who are separating, retiring, or whose access has been suspended for cause per reference (u), have completed a Security Termination Statement (STS).

(a) For military personnel, all completed STS must be forwarded to HQMC Manpower and Reserve Affairs (M&RA) (MMRP-20) for inclusion in the Official Military Personnel File (OMPF).

30 JAN 2017

(b) For civilian personnel, all completed STS must be forwarded to the appropriate servicing HR office.

(15) Ensures all personnel execute a **CLASSIFIED NATIONAL SECURITY INFORMATION NONDISCLOSURE AGREEMENT STANDARD FORM 312** prior to granting initial access to classified NSI. A hard copy shall be forwarded to HQMC M&RA (MMRP-20) for Marines and to the servicing civilian HR office for civilian employees, with the execution documented within JPAS.

(16) Periodically instruct members of the command's Force Preservation Council (FPC) what circumstances warrant the suspension of access to classified material or processing for revocation of security clearance."

5. Top Secret Control Officer (TSCO). Commands which handle Top Secret information/material shall designate, in writing, a TSCO.

a. The TSCO must be a Gunnery Sergeant (E-7) or above, or a civilian employee GS-7 or above.

b. The TSCO must be a U.S. citizen with a favorably adjudicated SSBI/T5 or SSBI/T5 Periodic Reinvestigation (T5R) within the previous 5 years.

c. The Command Security Manager may also be designated as the TSCO as a collateral duty.

6. Security Assistants. Commanding Officers may elect to assign additional security personnel depending on the size of the command, mission and particular circumstances. Assistants may include the following positions or others, depending on command requirements:

a. Assistant Security Manager. Persons designated as assistant security managers must be U.S. citizens, and either Staff Sergeant (E-6) or above, or civilians GS-6 or above.

(1) The designation must be in writing.

(2) Assistant Security Managers shall have a SSBI/T5 only if they are designated by the command to authorize Temporary Access (formerly Interim Access); otherwise, the investigative and eligibility requirements shall be determined by the level of access to classified NSI required.

30 JAN 2017

b. Security Assistant. Military, government civilians, and contractor employees performing administrative functions under the direction of the Command Security Manager may be assigned without regard to rank or grade as long as appointee has the appropriate eligibility necessary for the access or position sensitivity required to perform their assigned duties.

c. Top Secret Control Assistant (TSCA). Individuals may be assigned to assist the TSCO as needed.

(1) The designation shall be in writing.

(2) A person designated as a TSCA must be a U.S. citizen and either an officer, enlisted member E-5 or above, or civilian employee GS-5 or above.

(3) Appropriately established Top Secret clearance eligibility is required.

(4) Top Secret couriers are not Top Secret control assistants.

7. Contracting Officer's Security Representative (COSR). All commands which award contracts to industry requiring access to classified NSI by the contractor and employees, or which shall result in the development of classified NSI and/or equipment shall appoint, in writing, one or more qualified security specialists as COSR for security.

a. Details concerning this requirement are contained in Chapter 6 of this Order.

b. Contracts with SCI performance of work requirements must be coordinated with the Command SSO, approved by the Command's Senior Intelligence Officer (SIO) and sent to SSO Navy and the Intelligence-Related Contract Coordination Office (IRCCO) before SCI access is granted to contracted personnel.

8. Information System Security Manager (ISSM). ISSMs are privileged users, which are defined as individuals who have access to system control, monitoring, or administration functions. Individuals having privileged access require training and certification to IA Technical levels I, II, or III depending on the functions they perform. They must also be trained and certified on the operating system or computing environment they are required to maintain. They should be a U.S. citizen and must hold local access approvals commensurate

30 JAN 2017

with the level of information processed on the system, network, or enclave. They must have IT-I security designation. A person with privileged access must have a NACI/T1 and/or an initiated SSBI/T5.

a. ISSM responsibilities are outlined within reference (ac).

b. Commanding Officers shall appoint a separate SCI Information System Security Manager or Officer (ISSM/ISSO) in accordance with reference (j) when the command has an operational Joint Worldwide Intelligence Communications System (JWICS) or other SCI network.

9. Special Security Officer (SSO). The Commanding Officer or Senior Intelligence Officer of commands in the DON, which are accredited for and authorized to receive, process, and store SCI, shall designate, in writing, an SSO.

a. The SSO is the principal advisor on the SCI security program in the command and is responsible to the Commanding Officer for the management and administration of the program.

b. All SCI matters are referred to the HQMC SSO.

c. The Command Security Manager cannot function as the SSO unless authorized by DIRINT.

d. Although the SSO administers the SCI program independent of the Command Security Manager, the Command Security Manager must account for all collateral clearance eligibility and access determinations made on members of the command.

(1) Cooperation and coordination between the SSO and Command Security Manager is essential, especially for personnel security matters.

(2) The Command Security Manager and the SSO must keep each other apprised of changes in status regarding security clearance eligibility and command security program policies and procedures as they have an impact on the command's overall security posture.

e. The command security instruction shall delineate the duties of the Command Security Manager and the SSO to ensure proper coordination and to prevent gaps in coverage of program responsibilities.

30 JAN 2017

f. The duties and responsibilities of the SIO and SSO are identified in reference (j).

10. Inspections, Assessments, and Reviews

a. Commanding Officers are responsible for evaluating the security posture of their subordinate commands. This includes developing an understanding of challenges subordinate commands have regarding execution of the requirements of this program and promulgating all information obtained from senior level commands.

b. Commanding Officers shall conduct inspections, assessments, and reviews to examine overall security posture of subordinate commands. Inspections or reviews of subordinate commands shall be conducted annually unless operational commitments prevent such action. IGMC inspections are no-notice.

c. HQMC PS shall conduct inspections of subordinate commands as an augment inspector with the IGMC Unit Inspection Program (UIP) or Command Inspection Program and the Mission Assurance Assessment Team (MAAT), which focuses on installation Mission Assurance Programs.

(1) To ensure the effective operation of the IPSP throughout the Marine Corps, HQMC PS may, on occasion, conduct inspections separate from the IGMC and MAAT.

(2) HQMC PS shall conduct biennial inspections of the NATO Program on commands approved to hold NATO material.

(3) Assessments and Reviews may be requested by contacting the IPSP Manager at HQMC PS. Assessments and Reviews shall not be scheduled within 90 days of a scheduled inspection or after a command has been notified that they are pending a formal inspection.

(4) HQMC SSO shall conduct reviews/inspections of the SCI security program(s) annually, or as required.

d. A command IPSP self-inspection guide is provided in references (t) and (u). These checklists may be modified to meet local command needs.

(1) The IPSP inspection checklist, Functional Area (FA) 5510.3 is available on the IGMC webpage:

30 JAN 2017

<https://hqmc.usmc.afpims.mil/igmc/Resources/Functional-Area-Checklists/>

(2) The FA 5510.3 Checklist shall be used for all inspections initiated by HQMC and may be used by subordinate commands as the basis of internal inspection programs.

(3) Questions may be added to the FA 5510.3 Checklist, but no question may be deleted. It is important to note, the FA 5510.3 Checklist is only a point of departure. All requirements established in the references in this Order are inspectable.

(4) SCI security program checklists and Sensitive Compartmented Information Facility (SCIF)/Fixed Facility Checklists shall be used by HQMC SSO for annual inspections.

e. Inspections of the command's IPSP by HQMC PS shall be evaluated on an Effective/Ineffective scale. Issues discovered during the inspection shall be determined to either be a Finding or Discrepancy.

(1) A Finding is an issue that is a significant deviation from policy or one that creates a situation that could result in a compromise of classified NSI.

(2) A Discrepancy is usually an administrative issue that impacts the smooth functioning of the program, but does not normally cause a compromise. If the discrepancy can be corrected while the inspector is on site, it may not be included in the final report to the Commanding Officer.

(3) The final determination of Finding or Discrepancy shall be at the discretion of the inspector. Any incidents discovered during the inspection that have caused a compromise of classified NSI not already known to the command, may result in a rating of Ineffective, regardless of the total number of Findings or Discrepancies.

(4) Additionally, if an instance of compromise is discovered during an inspection, a Preliminary Inquiry must be initiated immediately per the provisions of reference (t).

11. Security Servicing Agreements (SSA). Commands may perform specified security functions for other commands via SSA. Such agreements may be appropriate in situations where security, economy, location, and efficiency are considerations.

30 JAN 2017

a. These agreements must consider the full spectrum of security services.

b. Considerations in developing the SSA include the capabilities and requirements of each participating command, and the command relationships that may or may not exist.

c. SSA shall be specific and must clearly define where the security responsibilities of each participant begin and end. The agreement shall include requirements for advising Commanding Officers of any matters which may directly affect the security posture of the command.

d. SSA should also include comments regarding funding for any additional inspections or Temporary Additional Duty (TAD) that may be incurred as a result of the agreement.

e. Append any SSA to the affected command security instruction.

12. Planning for Emergencies. All commands, squadron/battalion level and above, shall establish an EAP for the protection and removal of classified NSI under its control during emergencies.

a. Outside Continental United States (OCONUS) Commands and commands which deploy shall include an Emergency Destruction Supplement (EDS) to their EAP. EAPs should be fully coordinated with the command's All Hazards Plan and included in the command security program instruction.

b. EDS should be sufficiently generic as to support the destruction of classified NSI in any potential situation. Only those materials resident within the confines of the command shall be used/planned for to support the EDS. Appendix D applies.

13. Annual Reporting Requirements. Reference (t) mandates reporting several items of information to support the DON's requirement for oversight of the Marine Corps IPSP.

a. Commands's will utilize **AGENCY SECURITY CLASSIFICATION MANAGEMENT PROGRAM DATA STANDARD FORM 311** for annual submission. STANDARD FORM 311 can be downloaded at <http://www.gsa.gov/portal/forms/download/116190> in accordance with reference (k).

30 JAN 2017

b. Data shall be consolidated at the MARFOR/MCICOM level for all subordinate commands and submitted to HQMC PS no later than 45 days past the end of the previous fiscal year. Report Control Symbol 5510-22 (External RCS DD-INT(AR)1418) is assigned to this reporting requirement.

c. SCI security program reporting is submitted to HQMC SSO as required.

Chapter 3

Security Education

1. Basic Policy. Commanding Officers shall establish and maintain an active security education program to instruct all personnel in security policies and procedures, regardless of their position, rank or grade.

a. The purpose of the security education program is to:

(1) Ensure that all personnel understand the criticality of, and procedures for protecting classified NSI.

(2) Increase security awareness for personnel throughout the command.

b. The goal is to develop fundamental security habits as a natural element of each task.

c. Security training must be sufficiently diverse and interesting to ensure that it is not viewed as drudgery to complete.

(1) It must be tailored to the command and its particular security requirements based on references (k), (t), and (u).

(2) As with Rifle Range Safety Briefs, principles of good security are effective only if they can be recalled without effort in a situation requiring immediate action.

2. Responsibility

a. HQMC PS is responsible for policy guidance and is the final approval authority for all information and personnel security training modules intended for Marine Corps-wide implementation. Development of security education materials for use within commands are approved by local Commanding Officers provided they are in compliance with this Order and its references.

b. DIRINT via HQMC SSO is responsible for the management and oversight for the SCI security program to include policy guidance, training, and reporting.

30 JAN 2017

c. C4/CY is responsible for all cybersecurity training modules and requirements for Marine Corps-wide implementation.

d. Recruit Depots are responsible for indoctrinating military personnel with a basic understanding and definition of classified NSI and why and how it is protected. Civilian employees and contractor personnel employed by the Marine Corps for the first time, must also be given a basic security indoctrination brief by the employing activity.

e. Commanding Officers are responsible for security education in their commands; ensuring time is dedicated for training and awareness.

(1) Personnel in positions of authority, in coordination with the Command Security Manager, are responsible for determining security requirements for their functional area and ensuring personnel under their supervision understand the security requirements for their particular assignment.

(2) Continual training is an essential part of command security education and leaders/supervisors shall ensure security training is provided.

f. The Command Security Manager shall develop a comprehensive training plan for all personnel to include those specific requirements for security personnel.

g. The Command SSO shall develop a comprehensive SCI security training plan for all SCI indoctrinated personnel.

3. Minimum Requirements. The following are the minimum requirements for security education:

a. Indoctrination of personnel upon employment by the Marine Corps in the basic principles of security (reference (u) paragraph 4-5 applies).

b. Orientation of personnel who will have access to classified information or assignment to sensitive duties (including IT duties) at the time of assignment, regarding command security requirements (reference (t) paragraph 4-6 applies).

c. On-the-job training in specific security requirements for the duties assigned (reference (u) paragraph 4-7 applies).

30 JAN 2017

d. Annual refresher briefings for personnel who have access to classified information (reference (u) paragraph 4-8 applies).

e. Counterintelligence briefings annually for personnel who have access to information classified Secret or above (reference (u) paragraph 4-9 applies).

f. Special briefings as circumstances dictate (reference (u) paragraph 4- 10 applies).

g. Debriefing upon termination of access (reference (u) paragraph 4-11 applies).

h. A comprehensive listing of Marine Corps training requirements is available on the HQMC IPSP web-page:
<https://eis.usmc.mil/sites/hqmcppo/PS/PSS/Blog/default.aspx>

4. Training for Security Personnel. Members of the Command Security Management team must avail themselves of all possible training opportunities to ensure they are prepared to effectively manage the command's IPSP. The Center for Development of Security Excellence (CDSE) under DSS provides a significant listing of resident and non-resident security training via Security Training, Education and Professionalization Portal (STEPP):
<http://cdse.edu/stepp/index.html>.

a. Command Security Managers and Assistant Security Managers shall attend the Marine Corps Security Management Course within 180 days of appointment. Security Assistants of any grade are encouraged, but not required, to attend this course.

(1) The Security Management Course provides the minimum training necessary to establish and manage a command IPSP.

(2) The Security Management Course is offered by a Mobile Training Team (MTT) from HQMC PS and shall provide Marine Corps-specific information and discuss the day-to-day mechanics of managing a command's IPSP.

b. Prerequisites established for the Marine Corps Security Management Course shall be completed by all security management personnel within 30 days of assignment regardless of course attendance. These courses are available online. A listing of course prerequisites is available on the HQMC IPSP web-page:

30 JAN 2017

<https://eis.usmc.mil/sites/hqmcppo/PS/PSS/Blog/default.aspx>

c. The Marine Corps Security Management Course MTT shall be requested by the senior command desiring to sponsor a course; sponsorship shall be no lower than the MEF/regional MCI level. OCONUS commands shall coordinate directly with HQMC PS regarding scheduling to meet the training requirement.

(1) The course shall be conducted for a minimum of 15 personnel.

(2) The maximum number of attendees shall be negotiated based on the facilities available for training.

(3) Organizational requirements for hosting the course are available on the HQMC IPSP SharePoint site.

d. The Security Professional Education and Development (SPeD) Certification Program (reference (m)), is part of DoD's initiative to professionalize the security workforce.

(1) This initiative is intended to ensure that there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

(2) Implementation guidance and additional detail shall be provided via separate guidance.

e. SCI security training requirements may be obtained from HQMC SSO.

5. Resources

a. HQMC PS shall provide announcements, updates, references, security blog, training material, program development documents, desktop tools, frequently asked questions, security videos, and other items via the HQMC IPSP SharePoint site.

(1) These materials shall be used by commands across the Marine Corps to develop and/or enhance local security training programs.

(2) Effective training requires tailored and meaningful information specific to unit mission and circumstance.

30 JAN 2017

(3) Development of training at the HQMC level cannot be expected to meet local requirements. Therefore, the tools provided on this website are only a point of departure and shall form the foundation for a comprehensive unit security training program.

b. HQMC SSO shall provide SCI related security training and information as needed. With the exception of specific security training information provided by HQMC PS and HQMC SSO, all commands are responsible for providing and reporting security training as applicable.

c. Command Security Managers must be resourceful and must research other training opportunities to ensure the organizational training programs meet the commander's needs.

Chapter 4

Information Security

1. Basic Policy. Commanding Officers shall ensure that all classified NSI entrusted to their command is protected per the provisions of this Order and references.

a. Personnel assigned to the command permanently or TAD, shall not be granted access to such material unless appropriately cleared according to references (k), (t), and Chapter 5 of this Order.

b. A Need-to-Know determination shall be made by the Commanding Officer prior to granting access to classified material.

c. At no time shall rank and position be the sole considerations for granting access.

d. Classified NSI shall be stored only in General Services Administration (GSA) approved security containers, in approved areas, on accredited IT systems, and under conditions which prevent unauthorized persons from gaining access. This includes securing the material in approved equipment or facilities whenever it is not under the direct control of an appropriately cleared person, or restricting access and controlling movement in areas where classified NSI is processed or stored.

(1) Areas designated as Open Storage shall be designated, in writing, by the Command Security Manager or Commanding Officer, as restricted areas following the completion of a Physical Security Survey (PSS) conducted in accordance with reference (z).

(2) All personnel shall comply with the Need-to-Know policy for access to classified NSI.

e. Classified NSI is the property of the U.S. Government and not personal property.

(1) Military, government civilian employees, and contractors who resign, retire, or otherwise separate from the Marine Corps, shall return all classified NSI in their possession or in security containers over which they exercise control to the command from which received, or to the

30 JAN 2017

Nearest Marine Corps command prior to accepting final orders or separation documents.

(2) All courier cards and hand-carry authorizations shall be returned to the authorizing Command Security Manager or SSO, or to the Command Security Manager or SSO at the appropriate Command nearest the location of the Marine or civilian who is departing Naval Service.

2. Classification Management

a. All commands possessing or authorized to receive and maintain classified NSI shall develop a Classification Management Program that describes and supports creation, marking, control, dissemination, and destruction of classified material in accordance with reference (c).

b. Across the government, the majority of classification actions are derivative in nature. Any person with appropriately assigned clearance eligibility and approved access may act as a derivative classifier. To support this authority, reference (c) established several requirements to ensure a better process.

(1) Derivative classifier training shall be conducted and documented initially for anyone within a command who has access to classified NSI and biennially thereafter for as long as the individual has access to classified NSI. If refresher training is not conducted within 24-months, derivative classifier authority shall be suspended for that individual until the training is conducted.

(2) The name of the person creating the derivative document must be placed on the derivatively created document. Reference (k) provides specific guidance.

(3) Identification of multiple sources used to derivatively classify a document shall be included on or with the document and retained during its lifetime.

3. Applicability of Control Measures. Classified NSI shall be afforded a level of control commensurate with its assigned security classification level. This policy encompasses all classified NSI regardless of storage location or media (e.g., removable or removed classified hard disk drives, external hard drives, computers, disks, documents, etc.).

4. Top Secret Control Measures

30 JAN 2017

a. Commands with Top Secret information shall appoint in writing a TSCO to maintain a system of accountability (e.g., registry) of documents and other physical media (e.g., disk drives, and removable computer media).

b. TSCO'S shall:

(1) Obtain a **Record of Receipt** (Form 5510/15) from each recipient for Top Secret information distributed internally and externally.

(2) Enter into the command's registry all Top Secret information originated, derivatively created, reproduced, or received by the command.

(3) Ensure that inventories of Top Secret information are conducted at least annually or more frequently when circumstances warrant. As an exception, repositories, libraries or commands which store large volumes of classified material may limit their annual inventory to all documents and material to which access has been given in the past 12 months, and 10 percent of the remaining inventory.

(4) Annotate the record of receipt when the information has departed the command via any means (e.g., destruction, downgrading or declassification, etc.).

c. Production, control, safeguarding, transmission, destruction, and reporting of SCI classified Material is administered and managed by the DIRINT via the Command's SSO within the SCIFs.

5. Secret and Confidential Control Measures

a. Commanding Officers shall have a system of control measures that ensure access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which access occurs and to the nature and volume of the information. The system shall include technical (e.g., software, hardware, or firmware), physical (e.g., physical barriers, locks, security containers, Intrusion Detection System (IDS), etc.), and personnel control measures (e.g., investigations, access, need-to-know, visit certifications, etc.). Administrative control measures, which may include records of internal distribution, access, generation, inventory, reproduction, and disposition, shall be required when technical, physical, and personnel control

30 JAN 2017

measures are insufficient to deter and detect access by unauthorized persons. Except as otherwise specified, requests for waivers shall be submitted in accordance with Chapter 1, paragraph 6 of this Order.

b. Classified material, Secret and below, stored and maintained in an area designated as Open Storage requires no additional control provided the material does not leave the confines of the Open Storage area. Material taken from the Open Storage area must be controlled and accounted for until returned.

c. Classified material stored in a security container in an area designated as Closed Storage must be controlled and accounted for until returned.

d. Classified material stored in a GSA approved security container located outside of an area designated as a Level One, Two or Three Restricted Area, shall be inventoried a minimum of once per year (i.e., annual clean-out) and the inventory retained for the life of the document, plus two years. Reference (z) applies.

e. Best Practices. The following include, but are not limited to, best practices for control measures:

(1) Implement a Classified Material Control Center (CMCC) (e.g. security office or document control or secondary control point, etc.) program which provides for a mandatory review of classified material before it is printed. This has served to improve the marking of classified documents that are produced.

(2) Implement the tracking of hard copy classified information by creating a log that have the following information: Subject or Short Title, Date of Document, office/unit and ID number or number that set-up by the office for document tracking. This log may be used for the required classified information annual clean-out.

(3) Implement discrepancy tools which are used to keep track of things not in compliance with regulations and command procedures. (e.g., mail sent/received improperly, documents received not properly marked, media not properly marked.)

30 JAN 2017

(4) Implement quarterly "clean out" days for proper destruction of controlled unclassified information produced in the command.

6. Classified Hard Disk Drives (HDD). Classified HDD shall be inventoried and controlled with a locally developed control number and stored in a location suitable for the storage of the level of classification for the information contained on the HDD.

7. Working Papers. Working papers include classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents.

a. Commanding Officers shall establish procedures to account for, control, and mark all working papers in the manner prescribed for a finished document of the same security classification level when retained more than 180 days from date of creation or officially released outside the organization by the originator. Care should be taken to ensure source material is connected with the Working Papers so that at the 180-day point, appropriate markings and source material association can be made.

b. Working papers shall be:

(1) Dated when created.

(2) Conspicuously marked Working Papers on the first page in letters larger than the text.

(3) Marked centered top and bottom on each page with the highest overall classification level of any information they contain.

(4) Protected per the assigned classification level.

(5) Destroyed, by authorized means, when no longer needed.

c. Email, blog, and Wiki entries, bulletin board posting, and other electronic messages properly transmitted on classified networks within or external to the originating activity shall be marked as required for finished documents, not as working papers.

8. CUI Control Measures

30 JAN 2017

a. In accordance with reference (k), Vol. IV, CUI (i.e., For Official Use Only (FOUO)) is unclassified information that requires dissemination control to preclude unauthorized public release and unauthorized disclosure of the information.

b. The holder of CUI has the final responsibility for determining whether an individual has a valid need for access to the information.

c. CUI documents may be destroyed by any of the means approved for the destruction of classified NSI or by any other means that would make it difficult to recognize or reconstruct the information.

9. Reproduction

a. The proliferation of reproduction machines throughout the Marine Corps has compounded the problems associated with reproducing classified NSI. Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced, including by e-mailing, scanning, and copying, to the extent operational needs require.

b. Copying on a machine not designated/authorized for the level of the material would be spillage.

c. Top Secret information reproduced shall be added to the command's Top Secret control registry.

d. Records shall be maintained for a period of 2 years to show the number and distribution of all reproductions of Top Secret, Secret, and Confidential documents marked with special dissemination and reproduction limitations.

e. Controlled areas for classified reproduction shall be established. At a minimum, the reproduction equipment authorized for reproducing classified material shall be specifically designated and signs shall be prominently displayed on or near the equipment to advise users.

(1) A sign may read, for example, **"THIS MACHINE MAY BE USED FOR REPRODUCTION OF INFORMATION UP TO THE SECRET LEVEL."**

(2) Machines that are not authorized for the reproduction of classified material shall be posted with a warning notice such as **"THIS MACHINE IS LIMITED TO REPRODUCTION OF UNCLASSIFIED NATIONAL SECURITY INFORMATION."**

30 JAN 2017

(3) Reproduction machines shall be located in areas that are easily observable to ensure that only authorized copies are being made and the number of copies is kept to a minimum.

e. If the designated equipment involves reproduction processes using extremely sensitive reproduction paper, the paper shall be used and stored in a manner to preclude image transfer of classified NSI.

f. Reproduced copies of classified documents shall be afforded the same security controls as those required for the original documents.

g. Reproduced classified NSI must show the classification and other special markings which appear on the original material from which copied. All reproduced material shall be double checked and remarked when the markings are not clear.

h. Any samples, waste, or overruns resulting from the reproduction process, shall be safeguarded according to the classification of the information involved. This material shall be promptly destroyed as classified waste.

(1) Areas surrounding reproduction equipment shall be checked for classified material that may have been left on nearby desks or thrown in waste-baskets.

(2) In the event the machine malfunctions, it shall be checked to ensure that all copies have been removed.

(3) After reproducing classified material, the machine shall be checked to ensure the original and all copies have been removed.

i. When selecting reproduction equipment, use the Defense Logistics Agency, Document Services which is the DoD preferred provider for large acquisitions such as multi-year leases for copiers/printer/fax equipment used throughout the command or installation, according to reference (aa).

(1) All requests for new equipment shall be submitted to the Command Printing Officer (CPO) for review and approval prior to purchase or lease.

(2) For commands not supported by a CPO, forward the request to the following address:

Commandant of the Marine Corps (ARDE)
Attn: MCCPPMO
3000 Marine Corps Pentagon (Room 2B253)
Washington, DC 20350-3000

j. Ensure the command inspects equipment prior to removal from protected areas to ensure all copies have been removed.

k. Production, control, safeguarding, transmission, destruction, and reporting of SCI classified Material is administered and managed by the DIRINT via the Command's SSO within the SCIFs.

10. Electronically Transmitted Classified Information

a. Information obtained from classified information systems, such as Secure Internet Protocol Router (SIPR), must be reviewed to determine the proper classification or security marking to prevent inadvertent compromise. While some information available via classified networks may be unclassified, the assumption must not be made that the entire product, including attachments, is unclassified.

b. If information extracted from classified information systems is not marked properly, either through document or portion markings, contact the document's originator and return the document for proper classification markings.

c. If a classified document is received via electronic means and printed, the printed document shall be handled and controlled commensurate with the highest level of classification in the document.

11. Classified Documents on External Media. The contents of classified removable hard drives and all other external storage media should be inventoried through the use of Print Screen captures at regular intervals to ensure that, in the event of loss or compromise, an accounting of the documents on the device is available.

12. Security Violations. The Commanding Officer shall ensure a Security Inquiry (SI) is conducted, in accordance with the requirements outlined in references (k), (t), and Appendix I of this Order. When a loss or unauthorized disclosure of classified NSI, to include electronic spillages, is suspected, a SI is mandatory.

30 JAN 2017

a. Failure to follow procedures that prevent a loss or unauthorized disclosure also require a SI.

b. The purpose of the SI is to, at a minimum, determine and report within 10 duty days:

- (1) If a loss or unauthorized disclosure occurred.
- (2) Extent of the loss or unauthorized disclosure.
- (3) Potential damage to national security.

c. The Commanding Officer shall appoint, in writing, a command official, other than the Command Security Manager or anyone involved, either directly or indirectly with the incident, to conduct a SI. The command official shall have:

(1) Eligibility and access commensurate with the classification level of the information involved.

(2) The ability to conduct an effective, unbiased investigation.

d. The Command Security Manager or SSO, in conjunction with the appropriate legal authority, shall support the SI process to:

(1) Ensure the investigation is conducted.

(2) Ensure the appropriate actions are taken to negate or minimize damage to national security; and to prevent future violations.

(3) Upon the initiation of the SI, notify the local NCIS field office who shall determine their level of involvement.

e. Electronic spillages shall be reported to the command IAM to ensure the incident is properly reported in accordance with reference (k, Vol III) and this Order.

(1) SI shall be completed within 10 duty days of initial discovery of the incident.

(2) The SI shall be completed regardless of whether the Judge Advocate General Manual (JAGMAN) investigation is required. If NCIS assumes responsibility for the case, any SI

30 JAN 2017

or command investigative actions will be conducted only after consultation and concurrence by NCIS.

(3) Contact the next senior command in the chain of command if circumstances exist that would delay the completion of the JAGMAN.

f. The Commanding Officer shall immediately take corrective actions to prevent recurrence if the SI does not reveal a loss or unauthorized disclosure of classified NSI but does reveal a weakness in security practices or established security procedures

g. If the SI reveals a loss or unauthorized disclosure of classified information is likely to have occurred, and/or disciplinary action is being considered or recommended by the Commanding Officer, the command shall conduct a JAGMAN investigation.

(1) Reports of inquiries and JAGMAN investigations, at a minimum, shall be designated and marked as FOUO.

(2) Copies of all SIs and JAGMAN investigations shall be forwarded to HQMC PS.

13. Practices Dangerous to Security. Certain practices dangerous to security, while not reportable as security incidents, have the potential to jeopardize the security of classified NSI and material if allowed to perpetuate.

a. Examples of such practices include:

(1) Placing a paper recycling box next to a classified copier or placing burn bags next to unclassified trash containers.

(2) Stopping at a public establishment to conduct personal business while hand-carrying classified information.

(3) Failing to change security container combinations promptly when required.

b. These practices, when identified, must be promptly addressed by security management and appropriate changes made, actions taken, or training provided, to ensure the security of classified NSI.

14. Destruction of Classified Material. Commanding Officers shall establish procedures to ensure that all classified material intended for destruction is destroyed by authorized means and by appropriately cleared personnel.

a. An annual clean-out day shall be established where specific attention and effort are focused on disposition of unneeded classified material.

b. Destroy classified NSI no longer required for operational purposes per reference (k), Vol. 3, and this Order.

15. Foreign Disclosure. Although not strictly a security function, the Designated Disclosure Authority (DDA), Foreign Disclosure Officer (FDO), and Command Security Manager shall be informed of all incoming and outgoing foreign visits within the command. Command SSOs must be informed 24 hours in advance for all foreign visits within SCIFs.

a. All information, whether oral and/or written, shall be reviewed and approved for disclosure by the DDA. This information includes classified military information and CUI.

b. Those commands who sponsor a Defense Personnel Exchange Program (DPEP) or Foreign Liaison Officer (DPEP/FLO) must strictly adhere to the provisions of the Delegation of Disclosure Authority Letter (DDL) which defines the authorities and information access allowed for the DPEP/FLO.

(1) If the DDL does not specifically authorize it, the DPEP/FLO **SHALL NOT** be allowed to work inside an area designated as Open Storage unless the information contained within the space has been sanitized to include only that to which the DPEP/FLO is specifically authorized.

(2) Locating a DPEP/FLO in a classified workspace for convenience, without a need for access, is strictly prohibited.

Chapter 5

Personnel Security

1. Basic Policy. Requests for PSI shall only be submitted on individuals in cases where a bona fide requirement exists for access to classified NSI or occupation of a sensitive position/position of trust.

a. This must be substantiated by:

(1) Billet/MOS requirements.

(2) Current directive.

(3) PD.

(4) BIC.

(5) Permanent Change of Station/Permanent Change of Assignment (PCS/PCA) orders.

(6) Individual Augmentee (IA) billet orders.

(7) Public law or other policy manual.

b. The PSI shall not be submitted based on the following:

(1) Individual desire.

(2) Convenience.

(3) Prior investigation.

(4) To support infrequent facility access where an escort is feasible.

c. If a command determines that the duties and access requirements of a billet have changed and a bona fide need for an SSBI/T5 exists but the BIC in the Table of Organization (T/O) does not indicate an SSBI/T5 is authorized, as indicated by the letter "T" or "I" under the "SC" Column, a Table of Organization and Equipment Change Request (TOECR) is required.

(1) Total Force Structure Division (TFSD) forwards all TOECRs for investigation changes to HQMC PS for review and approval.

30 JAN 2017

(2) The TOECR must include clear justification regarding the need for the SSBI/T5 and should be coordinated with the Command Security Manager and SSO, if SCI access is desired, prior to submission.

(a) Justification must include the increased classified access requirements, Military Occupational Speciality (MOS) modifications, or other billet changes.

(b) Anticipation of future need is not sufficient to justify the modification of the BIC.

(3) Concurrence by HQMC PS is contingent upon articulated requirements and current funding levels. If denied, requests for reconsideration shall be entertained with additional justification for the investigation.

(4) Approval of the TOECR by HQMC PS must be obtained before the request for the SSBI/T5 is submitted via the Electronic Questionnaire for Investigations Processing (e-QIP).

(5) The BIC change does not need to reflect on the T/O before submission of the investigation as this can be a lengthy process.

d. MCSC is the acquisition command for the Marine Corps and is a CAO.

(1) BICs, billets and personnel may be moved from one program to another to support acquisition strategies throughout a program's life cycle.

(2) MCSC shall track their "T" coded BIC structure in their locally maintained CMT. SSBI/T5 level investigations shall only be initiated when absolutely necessary.

e. No individual shall be given access to classified NSI or be assigned to sensitive duties unless a favorable personnel security determination has been made regarding their loyalty, reliability, and trustworthiness. A PSI is conducted to gather information pertinent to these determinations. Exceptions to this requirement are outlined in reference (u).

f. Only the following officials are authorized to request PSI's on individuals under their jurisdiction:

(1) Commanding Officers.

- (2) Director, DODCAF DON.
- (3) CG, MCRC.

g. The scope of the investigation conducted shall be commensurate with the level of sensitivity of the access required or position occupied. Only the minimum investigation to satisfy known requirements may be requested.

h. The minimum investigation for enlistment or appointment in the Marine Corps is NACL/T3. This investigation is initiated on all prospective Marines by MCRC during the accessions process. CG, MCRC and CG, TECOM are tasked as previously stated in the execution statement in this Order.

i. There are rare instances where the investigation may not be completed prior to the Marine reaching his first assignment and, in some cases, there may be no record of the investigation ever being initiated. To ensure compliance with reference (u), all commands shall review the JPAS Person Summary Screen for all Marines joining the unit. The following actions shall be taken:

- (1) NACL/T3 shows complete with adjudicative decision indicated. No action required.

- (2) NACL/T3 shows open but not complete.

- (a) Monitor to ensure completion and adjudication within 180 days of opening.

- (b) Beyond that date, submit a Request to Research/Upgrade (RRU) to DODCAF DON and request status and adjudication.

- (c) If the Marine shall depart the command before the 180 day mark, input an entry in JPAS under "REMARKS" concerning the actions taken on the file. This shall prevent unnecessary duplicative action on the part of the next command.

- (3) No indication of NACL/T3 submission. Contact OPM to determine status of investigation. If no evidence of NACL/T3, submit request for NACL/T3.

j. OPM conducts (or controls the conduct of) all PSI's for the Marine Corps.

30 JAN 2017

(1) Marine Corps elements are prohibited from conducting PSI's, including local public agency inquiries.

(2) An exception to this restriction is made for Marine Corps overseas commands employing foreign nationals for duties not requiring access to classified NSI. Reference (u) provides further details.

(3) Marine Corps commands may not obtain credit reports or civilian criminal history files for any individual for the purpose of making decisions regarding eligibility or potential eligibility for access to classified information.

k. Reference (u) states that PSI's and PRs shall not be requested for any civilian or military personnel who will retire, resign, or separate with less than one year service remaining.

(1) Fiscal constraints and overburdened investigative agencies prevent the submission of all but essential requests for investigation.

(2) Exceptions shall be granted only for those personnel whose participation in a Special Access Program (SAP) is documented with appropriate orders and whose continued assignment is contingent upon completion of the required PR.

(3) Submission of a request for investigation to ensure current eligibility following departure from Naval Service is expressly prohibited.

l. Validation of current billet clearance eligibility status is required prior to awarding access to classified NSI and must be determined prior to submitting a PSI.

(1) Consult JPAS. JPAS is DoD's system of record for personnel security issues and maintains current investigative and eligibility data.

(2) If JPAS is not available, contact the DODCAF DON to determine current eligibility and the investigative basis prior to making access decisions. Ensure that accurate records are kept to facilitate updates to JPAS when it becomes available.

m. Administrative termination of access at the losing command is required when a Marine executes PCS/PCA orders or a government civilian employee transfers within the DoN.

30 JAN 2017

(1) Removal of access must be annotated in JPAS with the appropriate reason being annotated from the drop down menu. This must be completed in conjunction with routine JPAS out processing procedures and command debriefings as required by reference (u).

(2) No action is required regarding clearance eligibility and the Security Termination Statement (STS) is not completed. Reference (u) provides specific guidance relating to actions upon termination of service.

(3) The above debriefing actions do not apply to those SCI indoctrinated personnel under the rules of reciprocity when the gaining SSO has received authorization from the SIO to accept a Transfer-in-Status (TIS) per reference (j). Reciprocity of SCI access does not apply to those personnel who have been granted access to SCI under an exception, waiver or deviation per reference (p).

n. The Secretary of Defense determined that additional measures were warranted to increase the awareness of individuals who were entrusted with access to Top Secret information and/or indoctrinated into SAPs.

(1) In compliance, the statement below shall be read aloud and 'attested to', in the presence of a witness other than the person administering the brief. This attestation is not a legally binding oath and shall not be sworn to.

(2) Attestation administration is required only one time, usually when the original **CLASSIFIED NATIONAL SECURITY INFORMATION NONDISCLOSURE AGREEMENT STANDARD FORM 312** is signed.

(3) Commands are encouraged; however, to implement the attestation statement as a part of the command's annual security refresher training and apply it to all levels of clearance eligibility.

(4) No documentation or reporting is required, other than the JPAS entry; however, inspection visits may inquire into the procedures in place to implement this guidance.

Attestation Statement

I accept the responsibilities associated with being granted access to classified national security information. I am aware of my obligation to protect classified national security information through proper safeguarding and limiting access to individuals with the proper security clearance and/or access and official Need-to-Know.

I further understand that, in being granted access to classified information and/or SCI/SAP, a special confidence and trust has been placed in me by the United States Government.

2. Access

a. Requirements for access. Access to classified NSI shall be granted only when the following requirements have been met.

(1) Appropriate eligibility established by an authorized adjudication facility such as the DODCAF DON.

(2) Completion of the **CLASSIFIED NATIONAL SECURITY INFORMATION NONDISCLOSURE AGREEMENT STANDARD FORM 312**.

(3) Confirmation of Need-to-Know by the owner of the information. The owner of the information is generally accepted to be the commanding officer of the organization which possesses the information to which access is sought.

(a) Need-to-Know is not based on rank or position.

(b) Need-to-Know is based on a person's need to review information directly related to their duties and/or assignment.

(c) Commands should establish formal procedures to make Need-to-Know determinations for permanent personnel as well as visitors.

b. The decision to grant access to classified NSI and material is a local command responsibility and applies evenly to military, government civilian and contractor personnel.

(1) Access must not be granted automatically and may be granted at levels below that of current eligibility based on the command's Need-to-Know determination.

30 JAN 2017

(2) Having access at a previous command does not automatically bestow access at the current command whether TAD or permanently assigned.

(3) This is especially true with contractors who may have higher level accesses granted at their company or an alternate site. These individuals shall only be granted that access necessary to accomplish their assigned task and only as stipulated in the DD 254 described in Chapter 6 of this Order.

c. To facilitate potential access to NATO classified information, all DoD military and civilian personnel who are briefed on their responsibilities for protecting U.S. classified information shall be briefed simultaneously on the requirements for protecting NATO information in accordance with reference (k).

(a) A written acknowledgement of the individual's receipt of the NATO briefing and responsibilities for safeguarding NATO classified information shall be maintained.

(b) Do not annotate the NATO briefing under this circumstance in JPAS. Reference (o) applies.

d. If at any time, pressure is exerted by any person, to include those of senior rank, to obtain access to classified NSI or unescorted access to classified spaces, such action shall be immediately reported to the Commanding Officer of the organization for determination as to additional action and potential subsequent reporting to NCIS and/or the DODCAF DON.

e. Completion of the **SENSITIVE COMPARTMENTED INFORMATION NON DISCLOSURE AGREEMENT FORM 4414** shall be completed by all DoD military, civilian and contractor personnel who are briefed on their responsibilities for protecting SCI classified information.

3. Local Records Checks. The DON no longer requires local record checks as a part of the investigative process or before granting access to classified NSI.

a. However, commands are encouraged to review local records available to them as a part of the command's decision process prior to granting access to classified NSI. Sources may include:

30 JAN 2017

(1) The Service Record Book (SRB)/Officer's Qualification Record (OQR). A review of a Marine's service record is conducted to determine if Page 11, 12, or 13-type entries exist which might raise concerns with the Marine's ability to properly handle or safeguard classified NSI. While Non-judicial punishment and counseling issues are not disqualifying in and of themselves, the charges or counseling topic and frequency may raise concerns.

(2) Medical Records. Screening of medical records is conducted by medical personnel only.

(a) Information obtained through this review is deemed appropriate for use in access determinations only if it raises questions concerning trustworthiness, judgment or reliability.

(b) This determination may only be made by a medical professional.

(c) This information may not be deemed derogatory if the information is derived through counseling based on service in a combat zone, marital or grief counseling, and not related to violence by the subject.

(3) Command drug and alcohol screening records.

(4) Installation Provost Marshal records, to include the Consolidated Law Enforcement Operation Center (CLEOC).

(5) Delinquency reports for the Government Travel Charge Card (GTCC). Delinquency reports should be provided to the Command Security Manager on a monthly basis to facilitate screening for all personnel with eligibility for access to classified NSI.

4. Temporary Access. Temporary Access is an interim measure designed to allow commands to grant access to classified NSI in instances where the required investigation is not yet complete. Requirements for Temporary Access are contained in reference (u).

a. Temporary Access shall not be an automatic response to situations where individuals do not possess eligibility at higher levels. Rather, risk management principles shall be applied to each situation. Temporary Access may be granted only

if the required investigation is submitted to OPM. Commands must ensure the investigation is monitored for completion.

b. In cases where potentially disqualifying information exists in the SF 86 or local files, Temporary Access shall not be granted. Potentially disqualifying information equates to that information which matches one or more of the 13 Adjudication Guidelines found in Appendix G of reference (u).

c. There may be instances where individuals report to a command and require access but are without the appropriate eligibility. In cases where there is an open investigation but no e-QIP file copy or SF 86 to satisfy reference (u) review requirements for Temporary Access, the **Collateral Temporary Access Screening Checklist NAVMAC Form 5527/1** may be utilized as a means to screen the individual and determine whether Temporary Access is warranted.

(1) The **Collateral Temporary Access Screening Checklist NAVMAC Form 5527/1** shall be signed by the individual and screener and maintained in the individual's security file until the open investigation is favorably adjudicated.

(2) If the investigation is found to be unfavorable and individual has been less than candid in answering the questions on this form, consideration may be given to action under the Uniformed Code of Military Justice (UCMJ) as this may be an indicator that the individual intentionally falsified documents in order to improperly gain access to classified NSI.

d. Temporary Access may not be used as a method to circumvent proper procedures or grant access to someone who is otherwise not eligible for such access.

e. DIRINT, via the Commanding Officer, may authorize temporary SCI access for military, civilian or contractor personnel when the following conditions are met:

- (1) Member does not possess dual or foreign citizenship.
- (2) Member is granted Interim SCI eligibility from the DoD CAF.
- (3) Member has a current or open SSBI/T5.
- (4) Member has no derogatory information revealed on their SCI Pre-Screen interview.

30 JAN 2017

(5) Member has no non-U.S. citizen immediate family members.

(6) Member has an established Need-to-Know.

f. In accordance with DON MEMO of 30 Apr 09 and DON BANIF 020-03, SCI exception packages will be forwarded to HQMC SSO for members with non-U.S. citizen immediate family members and will be based on an assessment of the country risk assessment and need for the members' services.

5. Types of Personnel Security Investigation. The following categories of personnel are associated with particular types of investigation(s):

a. Military personnel.

(1) Fingerprint Special Agreement Check (SAC). This is the fingerprint check used for higher level investigations. On occasion, this may be the only investigation on file in JPAS; and in some instances may be recorded as "Expanded National Agency Check (ENAC)." If this is the case, the command must submit the Marine for a T3 regardless of access or MOS requirements. Neither the ENAC nor SAC support access to classified NSI or enlistment suitability requirements.

(2) NACLC/T3. This investigation forms the basis for enlistment/appointment suitability and must be completed on all Marines, officer and enlisted. The NACLC/T3 is submitted by MCRC as a prerequisite for shipping a recruit or officer candidate. The NACLC/T3 establishes Secret eligibility if adjudicated favorably.

(3) SSBI/T5. The SSBI/T5 shall only be submitted on those Marines who require access to Top Secret and/or SCI information, have fiduciary responsibilities and/or meet other critical sensitive or special sensitive requirements as defined in reference (u), or who are assigned as Network Administrators in an IT Level 1 position.

(a) These billets must be annotated in the Total Force Management System (TFMS) with the appropriate designation evident in the BIC and visible on the unit Table of Organization (TO).

(b) If a SSBI/T5 is required for any billet or individual not coded in TFMS, the command shall submit a TOECR

30 JAN 2017

via their appropriate chain of command to Total Force Structure Division (TFSD).

(c) The command may initiate the appropriate investigation upon confirmation from TFSD that the TOECR request has been approved. Though any Command Security Manager may submit a request for a SSBI/T5, Single Scope Background Periodic Reinvestigation (SSBI-PR)/(T5R), and/or Phased Periodic Reinvestigation (PPR), any SSBI-PR/T5R/PPR submitted specifically for the purpose of obtaining SCI access must be pre-screened by the servicing SSO to determine suitability for such access and to ensure all required documentation is submitted.

b. Government Civilian Employees.

(1) NACI/T1. The NACI/T1 is an investigation mandated by reference (r); is required to determine government employment suitability; and must be completed on every government civilian employee. NACI/T1 is also the minimum level investigation necessary to support issuance of the Common Access Card (CAC). If an employee requires access to classified NSI, employment suitability requirements per reference (s) are satisfied with the submission of an ANACI/T3 or SSBI/T5.

(2) ANACI/T3. Favorable adjudication of the ANACI/T3 supports the assignment of Secret eligibility and suitability for assignment to non-critical sensitive positions for civilian employees.

(a) The ANACI/T3 meets all requirements to establish clearance eligibility and government employment suitability.

(b) T3 investigation must be submitted for military personnel who retire or separate from the military and become employed as a federal civilian servant as a first time employee, unless the member was previously subject to a SSBI/T5.

(c) If a Marine becomes a civilian employee and has a valid, in-scope T3, with Secret eligibility on file, this shall be sufficient to retain eligibility and meet government employment suitability requirements.

(d) The investigative standard for government civilian employees requiring a Periodic Reinvestigation (PR) supporting access to Secret classified NSI is the T3R.

30 JAN 2017

(3) SSBI/T5. The SSBI/T5 shall only be submitted on those civilians who require access to Top Secret and/or SCI information, have fiduciary responsibilities and/or meet other critical sensitive or special sensitive requirements as defined in reference (u), or who are assigned as Network Administrators in an IT Level 1 position.

c. Contractors. Commands and organizations shall not submit requests for investigation on contractors with the exception of those necessary for issuance of the CAC. If a contractor requires a CAC for authorized purposes and does not require access to classified NSI, the command shall submit the NACI/T1 to satisfy CAC vetting mandates per reference (q).

(1) All investigations necessary to meet contract requirements for access to classified NSI shall be submitted by the contractor's Facility Security Officer (FSO). An exception exists for those contractors who require an investigation to support IT level I, II, or III requirements.

(2) If access is not otherwise required, the command shall submit the request for investigation to support the appropriate level of IT access.

d. Formal School Instructors. Persons selected for duties in connection with formal programs involving the education and training of military or civilian personnel must have a favorably adjudicated NACLC/ANACI/T3/T3R prior to assignment.

(1) This requirement applies to those assigned to formal programs and does not include those incidentally involved in training.

(2) It does not apply to teachers or administrators associated with university extension courses conducted on DoN installations in the United States.

e. Non Appropriated Fund (NAF) Employees. NAF employees may be the subject of a PSI if their particular duty assignment requires access to classified NSI or if their duties are considered sensitive. To support the submission of the PSI, the individual's PD must annotate such a requirement. PSIs shall not be submitted on NAF employees simply for temporary access to classified spaces.

f. Consultants. Consultants are treated, in terms of PSI submission, as government employees. However, a valid agreement

30 JAN 2017

must be in place between the individual and the Marine Corps to support requests for investigation.

6. Adjudicative Entries. The DODCAF DON shall assign eligibility at the highest level supportable by the most recent investigation favorably completed. If an SSBI/T5 is submitted on an individual, without disqualifying information to the contrary, the DODCAF DON shall adjudicate that investigation at the SCI level.

a. Potential DODCAF DON adjudicative entries shall include:

(1) Confidential. The individual may only access information and material at the Confidential level.

(2) Secret. The individual may have access to Confidential or Secret information and material.

(3) Top Secret. The individual may have access to Confidential, Secret, and Top Secret information and material.

(4) SCI. Access at the SCI level is determined by the Command's servicing SSO and is not within the authority of the Command Security Manager. However, all SCI access decisions must be communicated to the Command Security Manager.

(5) No Determination Made. This may be entered in cases where questions exist that prevent immediate adjudication of the investigation. Concerning questions of clearance eligibility, this entry shall typically be made only after the DODCAF DON has attempted to contact the command for resolution.

(a) Access to classified NSI and assignment to sensitive duties is not authorized with this entry.

(b) Commands must engage with the DODCAF DON to resolve this entry; it may not remain in a file indefinitely.

(6) Favorable. This may be entered when security clearance eligibility cannot be readily established. "Favorable" indicates the individual has a generally favorable investigation but either has minor issues requiring a suitability determination, or has other issues such as non-U.S. citizenship, which may allow employment but would not support establishing security clearance eligibility.

30 JAN 2017

(a) If clearance eligibility is required, submit a RRU to the DODCAF DON via JPAS to request eligibility. Access to classified NSI is not authorized with this entry.

(b) This entry may also be present as the result of the NACI for employment suitability purposes and for contractors suitable for issuance of the CAC.

(7) Pending Action or Requires Review. These entries indicate the existence of derogatory or adverse information. Submit an RRU to DODCAF DON via JPAS to request an eligibility determination and to determine what information is required. Access **MAY NOT** be granted.

(8) Loss of Jurisdiction. This entry indicates that an individual changed their employment status (e.g., from active duty to Individual Ready Reserve (IRR), civilian, or contractor; from one service to another, etc.) while in the process of adjudication.

(a) When jurisdiction is lost, the completed investigation shall not be adjudicated by the previous, cognizant adjudication facility.

(b) If a security clearance eligibility determination is required, verify no break in service over 24 months, and then contact the DODCAF DON via RRU to ask for an eligibility determination.

(c) Access **MAY NOT** be granted until resolved.

b. Entries from paragraphs (5), (7), and (8) above must be resolved by contacting the DODCAF DON to determine what they require in order to render a decision. Failure to do so prevents the commander from granting access to classified NSI to the individual and potentially withholds information on the individual that may result in administrative or judicial action related to derogatory information contained in the investigative file.

(1) It is important to understand the potential downside of requesting an eligibility determination via RRU in cases where the candidate will have access to information other than Confidential, Secret, Top Secret, or Top Secret/SCI.

(2) If the request cannot be supported based on information in the file, the command may receive a Letter of

30 JAN 2017

Intent to Deny or Revoke eligibility. This process is detailed in paragraph 9 below.

c. Additional information may be obtained at the DODCAF DON website.

7. Continuous Evaluation Program (CEP)

a. Requirements and Reporting

(1) As directed in reference (u), Commanding Officers shall report questionable or unfavorable information that may be relevant to the 13 Adjudication Guidelines to the DODCAF DON regarding members of their command based on recommendations made by the Command Security Manager.

(a) Rumors and other information derived from individuals who may have ulterior motives shall not be reported unless substantiated.

(b) The threshold for reporting such information shall be the point where the Commanding Officer believes that the weight of the reported information is sufficient to warrant further investigation.

(c) Failure to report information under the CEP constitutes a violation of a lawful order. Military personnel are subject to punishment under the Uniform Code of Military Justice (UCMJ); civilian personnel may be subject to criminal penalties under applicable federal statutes, as well as administrative sanctions.

(2) Adverse information received per the provisions of the 13 Adjudication Guidelines, shall be reported on individuals via the JPAS Incident Report link to the DODCAF DON.

(a) This standard is applied to all Marines, Navy personnel assigned/attached to Marine Corps commands, government civilian employees, contractors, NAF employees and consultants.

(b) For contractors, the Command Security Manager shall coordinate with the contractor Facility Security Officer (FSO), providing all pertinent adverse/derogatory information for further FSO reporting to the DODCAF-Industry (DODCAF IND).

(c) Coordination must also be made with the COSR for the contract along with a decision by the Commanding Officer concerning continued access to classified material.

(d) The Command Security Manager and SSO shall coordinate their efforts to ensure reporting via JPAS and the submission of a "Security Access Eligibility Report" (SAER) on all personnel holding SCI access. Incident reports involving SCI classified information shall be reported to HQMC SSO.

(3) As indicated in reference (u), adverse reports shall be made without attempting to apply any mitigating conditions found in the adjudication standards. Initial incident reports are made in JPAS prior to the completion of any investigations that may or may not be anticipated.

(a) The rationale for such reporting is that the DODCAF DON is the only consolidated repository within the DoN for information of this nature.

(b) Reports which turn out to be unfounded require only a final report to that end.

(c) If individuals amass several reports concerning potentially disqualifying information overtime, the DODCAF DON may review the record for trends which would make the individual unsuitable to hold clearance eligibility.

(d) Without such reporting, individuals could be involved in questionable events across a career at various locations throughout the government. With no consolidated reporting process, there would be no analysis to review eligibility decisions over time.

(e) Reporting of relevant personnel information to Command SSOs for SCI indoctrinated personnel shall be in accordance with reference (j). Further reporting to SSO Navy via HQMC SSO may be required.

b. Sources of Information

(1) Sources of information for reporting under the CEP include, but are not limited to:

(a) Unit Punishment Book.

(b) GTCC Delinquency reports.

30 JAN 2017

(c) Self reporting.

(d) Information derived from leadership counseling.

(e) Unit alcohol and drug counseling records.

(f) Information reported by other members of the command.

(g) Blotter reports.

(h) Unit legal reports.

(2) Financial issues comprise the majority of the disqualifiers for clearance eligibility revocation and denial. As such, it is important that individuals with financial issues seek help immediately after an issue is identified.

(a) There is no way to hide from debt and the credit report is a key tool used by the DODCAF DON to make eligibility determinations.

(b) If issues arise, no cost financial services and counseling should be sought from Navy/Marine Corps Relief and the individual's financial services provider before engaging fee-based services which can increase cash outlay at a time when that is the least desirable option.

(3) Reporting of financial delinquencies to the DODCAF DON via JPAS shall be made when the debt becomes 90 days delinquent unless the Commanding Officer determines that the individual's delinquency is unavoidable.

(a) Poor planning on the part of the individual is not sufficient to invoke this exception.

(b) Additionally, the command must monitor the situation to ensure that progress is made on repayment of the debt.

8. Pre-Screening

a. In general terms, individuals may not be pre-screened for employment as these results in a decision that only the DODCAF DON can make.

30 JAN 2017

(1) Civilian employment hiring decisions may be contingent on the granting of specific eligibility required for the position provided that requirement is stated in the PD and/or job announcement. Employment termination may result if required eligibility is denied or revoked by the DODCAF DON.

(2) Civilians offered positions of trust requiring access to SCI who do not have the requisite security clearance eligibility at the time of the initial offer shall receive a pre-interview suitability screening by the SSO as part of the SSBI/T5 submission and adjudicative processes.

(3) Marines may, depending on assignment specific requirements, be screened for appropriate eligibility with orders denied or held in abeyance pending completion of appropriate investigations. SCI suitability screening completed by the SSO is required for all MOS assignments requiring SCI eligibility. The following instances apply:

(a) Suitability determinations. Suitability for government employment is determined by the conduct of a Tier 1/NACI.

1. This investigation is based on the SF 85 and, when completed, returned to the submitting command for a suitability determination.

2. These determinations are to be made by the command's supporting HR office. If the employee is found to be unsuited for government employment, the employment may be terminated.

3. It is important that the NACI/T1 be prepared and submitted immediately upon employment.

4. The request for investigation may be submitted upon receipt of a letter accepting the offered position and signed by the applicant.

(b) Special Duty Assignment Screening. Certain billets within the Marine Corps require specific skills, experience and clearance eligibility. In the event that a Marine is found to be missing the required eligibility, the appropriate request for investigation shall be submitted.

1. If the Marine is otherwise qualified for the assignment, the lack of eligibility should not be the deciding

30 JAN 2017

factor unless potentially disqualifying information is indicated on the request for investigation.

2. In these instances, every effort should be made to hold orders in abeyance pending completion of the investigation and decision by the DODCAF DON.

b. All personnel submitting requests for investigation should obtain a copy of their credit report to ensure that the information reported in the SF 86 is accurate and to proactively address credit issues.

(1) Commanding Officers shall not require anyone to produce a copy of the credit report or to obtain one for this purpose. However, educating personnel as to the value of this review can forestall many future problems.

(2) Free annual credit reports are available to everyone from the three major credit reporting agencies.

(3) Commands should encourage everyone to review these reports as a part of the overall Command Security Education Program.

9. Adverse Actions. The integrity of the personnel security process depends on accurate reporting from commands across the Marine Corps. In conjunction with these reports, the only other action that a command may take is to suspend an individual's access to classified NSI.

a. Only the DODCAF DON can take action on eligibility. This action is contemplated when compiled information suggests that a person's judgment, trustworthiness and reliability might be in question.

b. If the DODCAF DON makes this determination, they shall issue the following notices to the command.

(1) Letter of Intent (LOI) to Deny or Revoke. The LOI is usually the first notice that the DODCAF DON is contemplating action that may result in the revocation or denial of clearance eligibility. The Command Security Manager or SSO, for those with SCI access, must facilitate this process and fully explain the contents and requirements of the LOI to the subject to generate the proper response to the DODCAF DON.

30 JAN 2017

(a) Commanding Officers shall personally review the case and make a conscious decision to allow or suspend access to classified NSI upon receipt of the LOI.

(b) If access is to be suspended, no JPAS "Access Suspension" is required at this point. Simply remove access administratively in JPAS to facilitate reinstatement when the LOI issues are resolved.

(c) The issues of concern shall be outlined to give the subject sufficient detail to respond appropriately. The response to the LOI must address every issue and be supported by documentary evidence. This list may include, but is not limited to the following items. This list shall be driven by the requirements of the LOI.

1. Letters from creditors.
2. Payment receipts.
3. Court documents.
4. Divorce decrees.
5. Personal recommendations. These should focus on the issues present in the LOI.
6. Any other document that supports the claim that an issue is resolved.

(d) Often, collection agencies are not willing to provide supporting documentation to the subjects of their collection efforts until the debt is fully paid.

1. One option is to have the subject contact the collection agency utilizing a speaker phone and ask for a status with the command's security representative present.

2. The command representative can prepare an affidavit concerning the conversation and attach that document to the response to provide proof of a current status.

(2) Letter of Denial (LOD). The LOD is the DODCAF DON decision concerning retention, denial or revocation of clearance eligibility. There are usually three options; Grant eligibility, Grant Conditional Eligibility, or Deny/Revoke.

30 JAN 2017

(a) If granted conditionally, the DODCAF DON shall levy monitoring requirements on the owning command to ensure the individual continues to meet the conditions set for retention of eligibility.

(b) Periodic reporting shall be required to ensure updated information is provided on the status of the outstanding issues.

(c) Failure to meet these requirements shall usually result in eligibility revocation.

(3) Appealing a DODCAF DON decision. If the DODCAF DON issues an LOD revoking eligibility, all access to classified NSI must be suspended. The command must also remove individuals from sensitive duties.

(a) Detailed instructions shall be provided concerning appeal options and include a written appeal directly to the Personnel Security Appeals Board (PSAB) or a personal appearance before an Administrative Judge (AJ) of the Defense Office of Hearings and Appeals (DOHA).

(b) If the subject wishes a personal appearance before the DOHA, the AJ's determination is only a recommendation and is not binding on the PSAB. Regardless of which route is chosen, the PSAB is the final stop in the process.

(4) Marines whose access to classified NSI has been suspended for cause or whose eligibility for access has been revoked by the DODCAF DON shall not PCS/PCA until a final decision has been rendered regarding appeals of their case. Commands shall report suspension and revocation action to MMEA or MMOA as appropriate and request that PCS orders be held in abeyance pending final resolution of the appeal.

c. Instructions are provided in each of the aforementioned documents and must be followed closely. The command security representative should be someone who is very knowledgeable of security processes, sufficiently senior to be a seasoned leader and someone who can devote the necessary time to follow this process to completion.

(1) This individual must act as an advocate for the subject of the notice and is the only person authorized to contact the DODCAF DON.

30 JAN 2017

(2) The subject of the notice must not attempt to contact the DODCAF DON.

(3) Each letter shall provide instructions for requesting extensions in order to prepare the response. These extensions should be requested to allow the individual the maximum time possible to develop his responses.

d. Correspondence from the DODCAF DON to the Command must **NEVER** be shared with the individual to whom it pertains unless specifically directed by DODCAF DON.

(1) There are provisions under the Freedom of Information Act (FOIA) that allow the subject to request copies of their investigative file from the Office of Personnel Management (OPM) or other government agencies.

(2) These requests must be annotated to indicate that the reason is to respond to an LOI or LOD and that expedited service is requested. Otherwise, the response may be received too late to be of use in the proceedings.

10. JPAS. JPAS is the DoD System of Record for Personnel Security and is a key tool in the management of the Personnel Security Program. The following web address provides users with the most up to date information concerning the system and also contains links for logging into the system as well as training and user guides.

<https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS>

a. If a member of the command or an individual visiting the command does not appear in JPAS, access to classified NSI may still be allowed, provided verification of appropriate eligibility can be obtained. Contact with the DODCAF DON or the individual's parent command are appropriate options to make this determination.

b. Each command shall manage JPAS as a unit process and shall assign two JPAS account managers to ensure appropriate authorities are resident within the organization.

(1) These individuals are usually the Command Security Manager and Assistant Security Manager.

(2) Other accounts may be assigned based on the commander's guidance and unit mission.

30 JAN 2017

(3) Accounts created for access control purposes alone shall be "read-only."

c. JPAS accounts are created by the first account manager in the security management chain of command.

(1) JPAS accounts are only to be issued for individuals that have current Secret eligibility based on a NACLIC/T3/T3R and are required to access the system for the daily performance of their jobs.

(2) Numerous guides, instructions, classes (both classroom and online) are available to instruct individuals on the proper use of the various functions within the system, but it is incumbent on unit account managers to train the users on the various functions of the system.

d. JPAS System Access Request (SAR) shall be completed, reviewed, and signed by the Command Security Manager prior to allowing access. The following are key elements for the management of JPAS:

(1) When JPAS accounts are created, under no circumstances shall permissions be granted for the processing of investigation requests as this function has been replaced by e-QIP Direct.

(2) The SAR shall be maintained in local files for a period of one year following the termination of the user's JPAS Account.

(3) JPAS accounts must be terminated when the account holder no longer occupies a security related billet.

(a) Under no circumstances shall a JPAS account holder retain an active JPAS account upon departing the unit, even if the holder knows they shall be occupying a security billet at their next unit.

(b) There is no value to "longevity" with JPAS accounts.

(4) JPAS accounts shall not be shared. Each account is created specifically for the individual and no account holder shall allow another individual to independently open or make entries in his/her account.

30 JAN 2017

(5) Proper management of a command's personnel security program requires that all personnel permanently assigned to or working in the command be included in the Personnel Security Management Network (PSMNet).

(a) If the command has an Industrial Security Program, contractors working in areas under the authority of the command must also be in the PSMNet, usually in a servicing relationship.

(b) Personnel TAD to the command may also be included in the PSMNet at the discretion of the commander.

e. JPAS is not authorized as a means of submitting or managing requests for investigation. This function is accomplished by using the e-QIP Direct, which allows commands to submit requests for investigation directly to OPM.

f. JPAS Uses:

(1) Verify security clearance eligibility.

(2) Determine the status of a personnel security investigation (duplicated in e-QIP Direct).

(3) Record the execution of the **Classified National Security Information Non-disclosure Agreement (SF 312)**.

(4) Record Temporary Access authorizations.

(5) Record command authorized access.

(6) Process incoming and outgoing visit requests.

(7) Communication with the DODCAF DON.

(8) Facilitate CE reporting.

g. All issues, questions, and problems with JPAS should be addressed to the Command Security Manager at the next higher unit in the chain of command. If further assistance is required, the Marine Corps Personnel Security Manager, who acts as the Marine Corps JPAS Manager, should be contacted.

11. e-QIP Direct. e-QIP Direct is the next generation of automated applications designed to improve the efficiency of the Personnel Security Process. e-QIP submits requests for

30 JAN 2017

investigation directly to OPM and allows commands to effectively and efficiently track these submissions.

a. The HQMC Personnel Security Manager is the only individual authorized to grant access to the OPM portal. All requests for access should be sent via the chain of command to the MARFOR/MCICOM level Command Security Manager who shall then forward them to HQMC PS.

b. e-QIP Direct accounts are created in a hierarchical structure. The next senior Command Security Manager in the chain of command shall provide training and guidance regarding management of the account. Additionally, the next senior Command Security Manager in the chain of command shall ensure the proper management of the subordinate e-QIP agencies, to include user accounts and oversight reporting.

c. Training materials can be obtained from the OPM portal under the "Library" link and via the OPM training website. Future formal training materials/classes shall be forwarded to all concerned parties as they become available. The Marine Corps Security Management Course shall provide additional instruction in the use of e-QIP Direct.

(1) OPM training website for agency users and applicants:

<http://www.opm.gov/investigations/e-qip-application/web-based-training/>

(2) OPM Portal:

<https://apollo.opm.gov>

(3) e-QIP Form for applicants:

<https://www.e-qip.opm.gov/eqip-applicant/showLogin.login>

(4) CDSE STEPP website:

<http://cdse.edu/stepp/index.html>

Chapter 6

Industrial Security

1. Basic Policy. Commanding Officers shall establish an industrial security program within their command if the command engages in classified procurement or when cleared DoD contractors operate within areas under their direct control.

a. Reference (h) provides specific guidance for the release and sharing of classified NSI with authorized contractors. This Order implements the requirements of reference (h).

b. Command security procedures shall include appropriate guidance, consistent with references (i) through (k), and this Order, to ensure that classified NSI released to industry is safeguarded appropriately.

2. Contracting Officer Security Representative (COSR). The Commanding Officer shall designate, in writing, one or more qualified security specialists as a COSR.

a. The COSR is responsible to the security manager for coordinating with program managers and technical and procurement officials during all phases of the procurement process to ensure that security considerations are reviewed and implemented in compliance with established policy and to ensure that the Statement of Work (SOW) and the DD 254 Contract Security Classification Specification document are prepared properly.

b. The COSR shall ensure that all industrial security functions and requirements are accomplished when classified NSI is provided to industry for performance on a classified contract.

(1) The DD 254 shall be signed by the COSR. At no time shall DD 254s be accepted if found to be signed by the FSO or other contractor unless that DD 254 is for a subcontract. The DD 254 is invalid unless signed by the proper official.

(2) Copies of the appropriate DD 254 shall be provided to all commands who are recipients of services provided by a classified contract. If not otherwise provided, Command Security Managers shall contact the contract's originating command and obtain a copy of the original DD 254 and all amendments for all classified contracts that authorize contractors to have access to classified NSI within their

30 JAN 2017

commands to ensure validation of contractor security requirements and authorizations.

c. The COR shall ensure the DD 254 is signed by the SSO and approved by the DoN for any SCI related contracting in accordance with SECNAVINST C4200.35A.

3. Contractor access to classified NSI. The presence of contractors within a command with access to classified NSI must be supported by a valid DD 254 and a valid visit request which identifies the contract and the individuals who shall support the contract.

a. Verification of clearance eligibility shall be made via JPAS and verification of Need-to-Know shall be made via an approved DD 254.

b. Regardless of the contractor's reflected JPAS access level, a contractor may not be given access to classified NSI material unless they are contractually bound to protect that information, via a classified contract with corresponding DD 254, for that specific classified NSI, at the level indicated on the DD 254.

c. Access for contractors shall be determined by the Commanding Officer. At no time shall access entries in JPAS, made by the contracting company, be acceptable for the assignment of access to NSI at Marine Corps commands.

d. Contractors with Temporary Access established by the DoD Consolidated Adjudications Facility, Industry (DODCAF IND) may be granted access at the SECRET level without further review. Access at the Temporary Top Secret level is at the discretion of the Commanding Officer. In all cases, if the Commanding Officer has reason to believe the individual is not a good security risk, access to classified NSI at any level may be withheld.

4. COSR Training. The assigned COSR shall receive training within 30 days of assuming contracting officer security representative responsibilities. The Defense Acquisition University (DAU) provides a web-based course entitled "COR with a Mission Focus," course number 'DAU CLC106.' The course is available at the following website:

<https://acc.dau.mil/CommunityBrowser.aspx?id=31505>.

30 JAN 2017

a. Other training opportunities may be available through sister Services or other venues; however, some research may be required.

b. COSR certification must be renewed every 2 years to maintain currency with the Federal Acquisition Regulation (FAR).

5. Security training for contractors. Contractors who have access to classified NSI shall participate in a security education and training program. If their work is performed solely within the confines of a command, in support of a classified contract, they may reasonably be expected to participate in the command's security training program.

a. If duties are performed at both the command and contractor facilities, the contractor may participate in the contractor's security training program. Evidence of training participation must be furnished to the command to verify participation.

b. The contractor may be required to participate in command specific training to address command specific and/or local security requirements. Failure to participate or failure to provide evidence of participation shall be grounds for suspension of access to classified NSI.

6. CEP for Contractors. Contractors who are involved in issues which require reporting under CEP shall be reported to DODCAF IND.

a. The Command Security Manager or SSO shall coordinate with the contractor FSO, providing all pertinent adverse/derogatory information for further FSO reporting to the DODCAF IND.

b. The Command Security Manager shall also report the same information to DSS Personnel Security Management Office for Industry (PSMO-I). PSMO-I may be contacted by telephone (443)-661-1320, facsimile (443)-661-1140 or e-mail AskPSMO-I@dss.mil.

c. The Command Security Manager or SSO shall ensure the local DSS representative follows up with the FSO to ensure the adverse/derogatory information is reported. Reference (u) applies.

Chapter 7

North Atlantic Treaty Organization (NATO) Program

1. Basic Policy. The Marine Corps implements the requirements mandated in reference (o) for the receipt, retention, storage, and release and sharing of classified NATO information within the Marine Corps.

2. Responsibilities

a. Central U.S. Registry (CUSR) oversees the administration of the U.S. NATO Registry System and is the authority for the establishment of the Marine Corps NATO Sub-registry.

b. Marine Corps NATO/COSMIC/ATOMAL Sub-registry. The Assistant Deputy Commandant, Plans, Policies, and Operations (Security), maintains the Marine Corps NATO Sub-registry under the authority of the CUSR.

c. The Marine Corps IPSP Manager is the Marine Corps NATO Control Officer and is responsible for the oversight and management of the NATO Program within the Marine Corps.

d. The Marine Corps NATO Sub-registry Control Officer shall manage the program through the following actions:

(1) Conduct formal inspections of all Marine Corps NATO Control Points at least once every 24 months.

(2) Conduct formal inspections of Communication Centers supporting an ATOMAL Control Point.

(3) Ensure coordination with NATO Control Point Officers across the Marine Corps on all issues related to the NATO Program.

(4) Ensure maintenance of an accurate inventory of all COSMIC Top Secret (CTS), NATO Secret (NS), and Atomal documents held at all control points across the Marine Corps. With change of the NATO Sub-registry Control Officer a 100% inventory shall be conducted.

3. NATO Control Point

a. Upon request, the Marine Corps NATO Sub-registry Control Officer may designate Marine Corps field commands as NAT

30 JAN 2017

Control Points if they demonstrate a requirement to receive and maintain NATO classified material. Commands designated as NATO Control Points shall assign, in writing, a NATO Control Point Officer and alternate(s).

b. The NATO control point officer is responsible for the following:

(1) Managing the activity's NATO Control Point as prescribed by reference (o) and this Order.

(2) Maintain control and accountability of all NATO classified material issued on sub-custody from the Marine Corps Sub-registry.

(3) Brief and debrief personnel assigned to the control point as required by reference (o) and this Order.

(4) Provide the Marine Corps NATO Sub-registry Control Officer with a current listing of names and specimen signatures for control point personnel who are authorized to receive NATO classified material using DAAG Form 29.

(5) Maintain a current listing of personnel who are authorized access to NATO classified NSI and the level of access.

(6) Maintain records reflecting the current status and location of NATO classified material received for sub-custody from the Marine Corps NATO Sub-registry.

(7) Provide a semi-annual NATO classified material inventory to the Marine Corps NATO Sub-registry Control Officer. Whenever the NATO Control Officer is changed, a 100% inventory shall be conducted.

(8) Maintain required references for implementation of an effective NATO security program.

4. User Offices. A command which requires the use of NATO documents for a period of 30 days or less may be designated a NATO User Office.

a. The NATO information point of contact within the User Office shall possess current clearance eligibility and shall maintain an access roster of personnel within the office to verify NATO access and Need-to-Know.

30 JAN 2017

b. User Offices may only receive accountable NATO material from the Marine Corps Sub-registry or Control Point via receipt and must return that material to the Sub-registry or Control Point when no longer needed.

c. User Office reproduction or destruction of accountable NATO material is not permitted.

d. A User Office's inventory of NATO classified material is managed by the Sub-registry or Control Point.

5. NATO Information. NATO Information is information that has been generated by or for NATO, or member nation national information that has been released into the NATO security system.

a. The protection of this information is controlled under NATO security regulations and the holder determines access within NATO, unless the originator specifies restrictions at the time of release to NATO.

b. All categories of NATO classified material are equivalent to the same classification of U.S. material and shall be afforded the same level of protection. See Reference (o) for the NATO classification levels.

6. Access and Investigative Requirements. Access to NATO information requires favorable eligibility and the Need-to-Know at the same level as for access to U.S. classified NSI. As stipulated in reference (o), access to NATO classified NSI shall also require a supervisor's determination of the individual's Need-to-Know and possession of the requisite security clearance.

7. Briefing/Re-briefing/Debriefing. Personnel authorized access to NATO classified NSI shall receive the appropriate briefing, Re-briefing, and debriefing as prescribed by reference (o) and this Order. The completion of this briefing, re-briefing, and debriefing must be recorded and this record retained for one (1) year following the individual's transfer or reassignment.

a. Briefing. All personnel requiring access to NATO Classified Information based on a Need-to-Know shall receive a security briefing and a signed acknowledgment. Receipt of the NATO briefing shall be verified prior to granting access to NATO classified NSI. The original statement shall be retained within the Control Point or security office of the authorizing command

30 JAN 2017

and access annotated in JPAS. Briefings and acknowledgment forms may be found at the CUSR website.

(1) NIPRNET website:

<https://securecac.hqda.pentagon.mil/cusr/>

(2) SIPRNET website: [http://classweb.hqda-](http://classweb.hqda-s.army.smil.mil/cusr.)

[s.army.smil.mil/cusr.](http://classweb.hqda-s.army.smil.mil/cusr.)

b. No Need-to-Know. In accordance with reference (o), to facilitate potential access to NATO classified NSI, all personnel that require access to classified NSI and DO NOT have a Need-to-Know to access NATO Classified Information shall be briefed on their responsibilities for protection of NATO information.

(1) A written acknowledgement of the individual's receipt of the NATO briefing and responsibilities for safeguarding NATO classified NSI shall be maintained.

(2) Do not annotate the NATO briefing under this circumstance in JPAS.

c. ATOMAL Briefing. Personnel to whom ATOMAL access is to be granted, and those who require continued access, shall receive an initial briefing and annual Re-briefing to remind them of their responsibilities and the special concerns for ATOMAL information.

(1) Access to ATOMAL information shall be authorized by the Marine Corps Sub-registry, or NATO ATOMAL Control Point.

(2) The individual must receive the ATOMAL security briefing and complete a statement acknowledging receipt of the briefing. The acknowledgement is available at <https://securecac.hqda.pentagon.mil/cusr/>. This access shall be annotated in JPAS.

d. Re-briefing. Persons who require continued access to ATOMAL COSMIC, ATOMAL SECRET, and ATOMAL CONFIDENTIAL information must be re-briefed annually to remind them of their responsibilities and the special concerns for ATOMAL information. Record the annual re-briefing on the original briefing certificate. If the original briefing statement is not available, a new statement acknowledging receipt of the re-briefing shall be signed.

30 JAN 2017

e. Debriefing. All persons having access to NATO or ATOMAL information shall be debriefed when access is no longer required. A termination briefing shall remind personnel regarding responsibilities for continued safeguarding of whatever NATO and/or ATOMAL classified NSI to which they may have had access. The debriefing statement must be retained for one (1) year.

8. Control and Handling. The Marine Corps Sub-registry is responsible for the receipt, accounting, handling, and distribution of accountable information. NATO control points may assign local control numbers or use Marine Corps control numbers for tracking of a document during inventories and the biannual NATO inventory as required by reference (o).

9. Storage. NATO classified material shall be protected and stored in accordance with reference (o). NATO classified material, if filed in the same container as U. S. classified material, shall be filed separately. (Comingling of information/material is **NOT** allowed).

10. Reproduction and Extracts. Reproduction of NATO classified material, regardless of the classification, is prohibited without approval from the Marine Corps Sub-registry or originating Control Point. Marine Corps classified material containing extracted NATO classified NSI shall be marked, handled and declassified in accordance with references (k) and (o).

11. Transportation and Transmission. The Marine Corps Sub-registry or Control Points are the only offices authorized to send NATO classified material directly to individuals and/or activities outside the Marine Corps.

a. Authority to hand-carry any NATO classified material must be in accordance with reference (o).

b. A NATO courier certificate must be used when hand-carrying NATO classified NSI. An example may be found at the CUSR NIPRNET website:
<https://securecac.hqda.pentagon.mil/cusr/>.

c. The SIPRNET website is <http://classweb.hqda-s.army.smil.mil/cusr>.

30 JAN 2017

12. NATO on the SIPRNET. The Marine Corps Enterprise Network is accredited for the transmission of NATO classified NSI, up to Secret, over the SIPRNET.

a. The Approving Official (AO) for the Marine Corps SIPRNET shall ensure accreditation is maintained in accordance with reference (o).

b. All equipment authorized to process classified NSI (e.g., desktops, laptops, and servers) that may process NATO Secret information must be labeled, using DD Form 2881 NATO Secret (Label) found at www.dtic.mil/whs/directives/forms/eforms/dd2881.pdf

(1) Removable computer storage media that is authorized to hold NATO classified NSI does not need to be accountable on the annual NATO inventory.

(2) Only removable computer storage media that actually contains NATO classified NSI is accountable on the annual NATO inventory.

13. Electronic Mail (E-Mail). NATO classified NSI may be e-mailed within a local area network (LAN) or between LANs that are accredited to process NATO classified NSI in accordance with reference (o). It is the sender's responsibility to verify that the receiver is cleared for access to NATO classified NSI and has a Need-to-Know.

14. Destruction. All NATO Control Points shall annually review their NATO classified NSI to determine whether it may be destroyed. NATO material classified NATO Secret ATOMAL and above shall be destroyed only by the Marine Corps Sub-registry.

a. NATO classified NSI shall be destroyed using the same methods as U.S. classified NSI and in accordance with reference (o).

b. NATO Control Points shall be authorized to destroy NATO Secret and below information. All destruction certificates must be witnessed by two persons appropriately cleared to the level of information to be destroyed. Destruction certificates shall be forwarded to the Marine Corps Sub-registry.

c. Destruction certificates for CTS ATOMAL and NATO Secret ATOMAL shall be maintained at the control points for ten years.

30 JAN 2017

11 other destruction certificates shall be maintained for five (5) years.

15. Compromise. All suspected or possible compromise of NATO classified NSI shall be reported immediately to the Command Security Manager and Control Point Officer.

a. Commands shall inform the Marine Corps Sub-registry within 24 hours of the suspected or possible compromise of NATO classified NSI. Additionally, notify the local NCIS field office.

b. The command reporting the incident shall immediately conduct an investigation as required by reference (o). The investigation shall determine whether a compromise occurred.

c. All investigations shall be forwarded to the Marine Corps Sub-registry.

16. Espionage, Sabotage, Terrorism, and Deliberate Compromise. Information concerning a deliberate compromise of NATO/ATOMAL information, attempted or actual espionage directed against NATO/ATOMAL information, or actual or planned terrorist or sabotage activity against facilities or users of NATO classified NSI shall be reported immediately to the Marine Corps Sub-registry, NATO Control Point, and local NCIS field office.

Appendix A

Glossary

ACCM	Alternative Compensatory Control Measures
AJ	Administrative Judge
ANACI	Access National Agency Check with Inquiries
AO	Authorizing Official
BIC	Billet Identification Code
CAC	Common Access Card
CAO	Competency Aligned Organization
CDSE	Center for the Development of Security Excellence
CEP	Continuous Evaluation Program
CG	Commanding General
CI	Counterintelligence
CLEOC	Consolidated Law Enforcement Operation Center
CMCC	Classified Material Control Center
CMT	Competency Management Tool
COMSEC	Communications Security
COS	Chief of Staff
COSR	Contracting Officer Security Representatives
CPO	Command Printing Officer
CTS	Cosmic Top Secret
CUI	Controlled Unclassified Information
CUSR	Central United States Registry
DAU	Defense Acquisition University
DDA	Designated Disclosure Authority
DDL	Delegation of Disclosure Authority Letter
DIRINT	Director of Intelligence
DOD	Department of Defense
DODCAF	Department of Defense Consolidated Adjudications Facility
DODCAF DON	Department of Defense Consolidated Adjudications Facility, Navy Division
DODCAF IND	Department of Defense Consolidated Adjudications Facility, Industry
DOHA	Defense Office of Hearings and Appeals
DON	Department of the Navy
DPEP	Defense Personnel Exchange Program
DSS	Defense Security Service
DUSN(P)	Deputy Under Secretary of the Navy for Policy
EDS	Emergency Destruction Supplement
E.O.	Executive Order
EAP	Emergency Action Plan
e-QIP	Electronic Questionnaire for Investigations Processing

FA	Functional Area
FAR	Federal Acquisition Regulation
FDO	Foreign Disclosure Officer
FLO	Foreign Liaison Officer
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPC	Force Preservation Council
FSO	Facility Security Officer
GSA	General Services Administration
GTCC	Government Travel Charge Card
HDD	Hard Disk Drive
HQMC	Headquarters United States Marine Corps
HR	Human Resources
HSPD	Homeland Security Presidential Directive
IA	Individual Augmentee
IGMC	Inspector General of the Marine Corps
INFOSEC	Information Security
IRCCO	Intelligence-Related Contract Coordination Office
IRR	Individual Ready Reserve
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
IPSP	Information and Personnel Security Program
JAGMAN	Judge Advocate General Manual
JPAS	Joint Personnel Adjudication System
JWICS	Joint Worldwide Intelligence Communication System
LAN	Local Area Network
LOD	Letter of Denial
LOI	Letter of Instruction/Letter of Intent to Deny or Revoke
M&RA	Manpower and Reserve Affairs
MAAT	Mission Assurance Assessment Team
MARFORS	Marine Forces
MCICOM	Marine Corps Installations Command
MCInTP	Marine Corps Insider Threat Program
MCRC	Marine Corps Recruiting Command
MCSC	Marine Corps Systems Command
MOS	Military Occupational Speciality
MTT	Mobile Training Team
NACI	National Agency Check and Inquiries
NACLCL	National Agency Checks with Law and Credit
NAF	Non-Appropriated Fund
NATO	North Atlantic Treaty Organization
NCIS	Naval Criminal Investigative Service
NDA	Nondisclosure Agreement

NS	NATO Secret
NSI	National Security Information
OCA	Original Classification Authority
OCONUS	Outside Continental United States
OMPF	Official Military Personnel File
OPM	Office of Personnel Management
OQR	Officer's Qualification Record
PAS	Privacy Act Statement
PCA	Permanant Change of Assignment
PCS	Permanent Change of Station
PD	Position Description
PII	Personally Identifiable Information
PP&O	Plans, Polices, and Operations
PPR	Phased Periodic Reinvestigation
PR	Periodic Reinvestigation
PS	Security Division
PSAB	Personnel Security Appeals Board
PSD	Position Sensitivity Designation
PSI	Personnel Security Investigation
PSMNet	Personnel Security Management Network
PSS	Physical Security Survey
RBE	Remain Behind Element
RRU	Request to Research/Upgrade
SAC	Special Agreement Check
SAER	Security Access Eligibility Report
SAP	Special Access Program
SAR	System Access Request
SCI	Sensitive Compartmented Information
SECNAV	Secretary of the Navy
SI	Security Inquiry
SIO	Senior Intelligence Officer
SIPR	Secure Internet Protocol Router
SMO	Security Management Office
SOI	Security Office Identifier
SON	Security Office Number
SPED	Security Professional Education and Development
SRB	Service Record Book
SSA	Security Servicing Agreement
SSBI	Single Scope Background Investigation
SSN	Social Security Number
SSO	Special Security Officer
STEPP	Security Training Education and Professionalization Portal
STS	Security Termination Statement
TBS	The Basic School
TECOM	Training and Education Command

30 JAN 2017

TIS	Transfer in Status
TOECR	Table of Organization and Equipment Change Request
TFMS	Total Force Management System
T/O	Table of Organization
TFSD	Total Force Structure Division
TSCO	Top Secret Control Officer
TSCA	Top Secret Control Assistant
UCMJ	Uniformed Code of Military Justice
XO	Executive Officer

Appendix B

Definitions

1. Unless otherwise noted, these terms and their definitions are for the purposes of this Order.

a. Access. The ability and opportunity to obtain knowledge or possession of classified information.

b. Adjudication. The process of an examination of a sufficient amount of information regarding an individual to determine whether the individual is an acceptable security risk. A determination that a person is an acceptable security risk equates to a determination of eligibility for access to classified information and/or sensitive duty assignment.

c. Alternative Compensatory Control Measures (ACCM). Used when an Original Classification Authority (OCA) determines that other security measures (as detailed in this instruction) are insufficient for establishing "Need-to-Know" for classified information and where Special Access Program (SAP) controls are not warranted. The purpose of ACCM is to strictly enforce the "Need-to-Know" principle.

d. Assessment. Actions that test the efficiency of a program via review of the standards and/or orders to determine if it achieved the intended results.

e. Authorized Person. A person who has a Need-to-Know for the specified classified information in the performance of official duties and who has been granted an eligibility determination at the required level.

f. Classified NSI (or "Classified Information"). Information that has been determined to require protection against unauthorized disclosure in the interest of national security and is classified for such purpose by appropriate classifying authority per the provisions of E.O. 12958, as Amended, or any predecessor Order.

g. Classified Material. Any matter, document, product or substance on or in which classified information is recorded or embodied.

h. Clearance. A formal determination that a person meets the personnel security eligibility standards and is thus

30 JAN 2017

afforded access to classified information. There are three types of clearances: Confidential, Secret, and Top Secret. A Top Secret clearance implies an individual has been determined by an authorized adjudicative authority to be eligible for access to Top Secret, and has access to the same; a Secret clearance implies an individual has been determined to be eligible for Secret, and has access to the same; and a Confidential clearance implies and individuals has been determined to be eligible for access to Confidential, and has access to the same.

i. Compromise. An unauthorized disclosure of classified information to one or more persons who do not possess a current valid security clearance.

j. Communications Security (COMSEC). The protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. COMSEC includes: (1) Cryptosecurity, which results from providing technically sound cryptosystems and their proper use; (2) Physical security, which results from physical measures taken to safeguard COMSEC material; (3) Transmission security, which results from measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis; and (4) Emission security, which results from measures taken to deny unauthorized persons information of value which might be derived from the interception and analysis of compromising emanations from cryptoequipment and telecommunication systems (See definition for EKMS).

k. Confidential. A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe. (E.O. 12598, as Amended)

l. Continuous Evaluation. The process by which all individuals who have established security clearance eligibility are monitored to assure they continue to meet the loyalty, reliability and trustworthiness standards expected of individuals who have access to classified information. The monitoring process relies on all personnel within a command to report questionable or unfavorable security information that could place in question an individual's loyalty, reliability, or trustworthiness.

30 JAN 2017

m. Contracting Officer. A Government official, who, per the departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representatives of the contracting officer, acting within the limits of their authority.

n. Contracting Officer's Security Representative (COSR). A security specialist at a DON contracting command who has been appointed as a COSR and delegated authority on behalf of the command for the security administration of classified contracts. The COSR serves as the responsible official for any problems or questions related to security requirements and/or classification guidance for classified contracts.

o. Controlled Unclassified Information (CUI). Official information not classified or protected under E.O. 12958, as Amended, or its predecessor orders that require the application of controls and protective measures for a variety of reasons.

p. Counterintelligence (CI). Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or their agents, or international terrorist organizations or activities.

q. Cybersecurity. Prevention of damage to, protection of, and resoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality and non-repudiation.

r. Disclosure. Conveying classified information to another person.

s. Document. Any physical medium such as any publication (bound or unbound printed material such as reports, studies, manuals), correspondence (such as military and business letters and memoranda), electronic media, audio-visual material (slides, transparencies, films), or other printed or written products (such as charts, maps) on which information is recorded or stored.

30 JAN 2017

t. Eligibility. A determination made by a DoD Consolidated Adjudication Facility, based upon favorable review of a standardized personnel security investigation, that an individual meets EO 12968 National Security Adjudicative Standards and is therefore eligible for access to classified NSI or assignment/retention in sensitive national security duties, or other designated duties requiring national security investigation and adjudication.

u. Employee. A person, other than the President and Vice President, employed by, detailed or assigned to, an agency, including members of the Armed Forces; an expert or consultant to an agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of an agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of an agency as determined by the appropriate agency head.

v. e-Qip. The Electronic Questionnaires for Investigations Processing is a software system developed by OPM which allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency or security management office for review and approval of the personnel security investigation request.

w. For Official Use Only (FOUO). A marking applied to unclassified information that meets one or more exemptions of the FOIA under Title 5 U.S.C., Section 522 (b) (2) through (9). Information must be unclassified to be designated FOUO. Declassified information may be designated FOUO, if it qualifies under exemptions 5 U.S.C. 522 (b) (2) through (9).

x. Information Security. The system of policies, procedures, and requirements established under the authority of E.O. 12958, as Amended, to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

y. Information System Security Manager (ISSM). Responsible for the cybersecurity program for a DoN information system or organization. This individual is responsible for creating the site accreditation package. The ISSM functions as the Command's focal point on behalf of and principal advisor for cybersecurity matters to the Authorizing Official (AO). The ISSM reports to the DAA and implements the overall cybersecurity program.

30 JAN 2017

z. Information Technology System. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception data or information. This includes computers, ancillary equipment, software and firmware.

aa. Inspection. Any effort to evaluate an organization or function by any means or method, including special visits, technical inspections, special one-time inspections, command assessments, inspections required by law or for the exercise of command responsibilities, and inspections conducted by higher headquarters staff.

ab. National Agency Check (NAC). A review of records of certain national agencies, including a technical fingerprint search of the files of the Federal Bureau of Investigation.

ac. National Agency Check and Inquiries (NACI). A review of documents and records conducted by the Office of Personnel Management (OPM), including a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references, schools and financial institutions.

ad. National Agency Checks with Law and Credit (NACLIC). The personnel security investigative requirement developed under EO 12968 for persons who will require access to Secret and Confidential classified information. A NACLIC covers the past 5 years and consists of a NAC, a financial review, certification of date and place of birth, and LACs. The NACLIC is the minimum investigative requirement for military service, and is the reinvestigative requirement for continued access to Secret and Confidential classified information (sometimes previously referred to as a Secret PR (SPR) or Confidential PR (CPR)).

ae. Access National Agency Check with Inquires (ANACI). This is a new investigation designed as the required initial investigation for Federal employees who will need access to classified NSI at the Confidential or Secret level. The ANACI includes NACI and Credit coverage with additional local law enforcement agency checks.

af. National Industrial Security Program. National program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the U.S. Government and serves as a single, integrated, cohesive

30 JAN 2017

industrial security program to protect classified information and preserve U.S. economic and technological interests.

ag. Need-to-Know. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized U.S. Governmental function.

ah. Nondisclosure Agreement (NdA). An agreement between an individual who will be permitted access to classified NSI and the United States government, acknowledging and agreeing to obligations for protecting classified NSI. All personnel must execute the Standard Form 312 Nondisclosure Agreement as a condition of access to classified information.

ai. Personally Identifiable Information (PII). Information used to distinguish or trace an individual's identity such as their name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personal, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with their personal or identifying information.

aj. Personnel Security Investigation (PSI). Any investigation conducted for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the DoD, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties or access requiring such investigation. PSIs are conducted for the purpose of making initial personnel security determinations and to resolve allegations that may arise subsequent to a favorable personnel security determination to ascertain an individual's continued eligibility for access to classified information or assignment or retention in a sensitive position.

ak. PSAB. The Personnel Security Appeals Board (PSAB) is the appellate authority for appeals of unfavorable DODCAF DON eligibility determinations.

al. Reciprocity. Acceptance by one agency or program of a favorable security clearance eligibility determination, made by another. Reciprocity does not include agency access determinations or employment suitability determinations.

30 JAN 2017

am. Record. All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by any command of the U.S. Government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that command or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the information value of data in them.

an. Reinvestigation. An investigation conducted for the purpose of updating a previously completed investigation of persons occupying sensitive positions, afforded access to classified information or assigned other duties requiring reinvestigation. The intervals of reinvestigation are dependent upon the sensitivity of the position or access afforded. A periodic reinvestigation of an SSBI/T5 is conducted at five-year intervals; a reinvestigation of a NACLIC/T3 for Secret or Confidential access is conducted respectfully at 10 year and 15 year intervals.

ao. Review. The evaluation of organizational processes and procedures in view of standing orders, policies, documentation, and other evidence with the purpose of reporting on the efficiency of a program, or more clearly defining an issue.

ap. Safeguarding. Measures and controls prescribed to protect classified information.

aq. Secret. A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe (E.O. 13526).

ar. Security. A protected condition that prevents unauthorized persons from obtaining classified information of direct or indirect military value. This condition results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influence.

as. Security Violation. Any failure to comply with the regulations for the protection and security of classified material.

at. Self-Inspection. The internal review and evaluation of a command or the DoN as a whole with respect to the

30 JAN 2017

implementation of the program established under E.O. 13526, and its implementing directives.

au. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources or methods, or analytical processes, that are required to be handled within formal access control systems established by the Office of the Director of National Intelligence.

av. Sensitive Duties. Duties in which an assigned military member or civilian employee could bring about, by virtue of the nature of the duties, a material adverse affect on the national security. Any duties requiring access to classified information are sensitive duties.

aw. Sensitive Information. Any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DON payroll, finance, logistics, inventory, and personnel management systems. Examples include FOUO, Unclassified Technical Data, State Sensitive but Unclassified (SBU), or Foreign Government information.

ax. Sensitive Position. Any position so designated, in which the occupant could bring about, by virtue of the nature of the position, a materially adverse affect on the national security. All civilian positions within the DoD are designated special-sensitive, critical sensitive, noncritical-sensitive, or non-sensitive.

ay. Significant Derogatory Information. Information that could, in itself, justifies an unfavorable administrative action, an unfavorable security determination, or prompts an adjudicator to seek additional investigation or clarification.

az. Single Scope Background Investigation (SSBI/T5). A personnel security investigation which provides extensive information regarding an individual, gathered from people and places where the individual has lived or worked. The period of investigation for a SSBI/T5 is variable, ranging from 3 years for neighborhood checks to 10 years for local agency checks. No

30 JAN 2017

investigative information will be pursued regarding an individual's life prior to their 16th birthday.

ba. Special Access Program (SAP). Any DoD program or activity (as authorized in E.O. 13526) employing enhanced security measures (e.g., safeguarding or personnel adjudication requirements) exceeding those normally required for classified information at the same classification level which is established, approved, and managed as a DoD SAP.

bb. Spillage. Occurs when data is placed on an IT system possessing insufficient information security controls to protect the data at the required classification. Electronic spillage resulting in the compromise of classified information is subject to the requirements of this Order.

bc. Survey. The process of gathering information, without detailed verification, on an entity or function being investigated or inspected, for the purpose of identifying problem areas warranting additional review or to obtain information for use in planning and accomplishing an investigation or inspection.

bd. Top Secret. A classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security, that the OCA is able to identify or describe (E.O. 13526).

be. Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

bf. Waiver. A written temporary relief, normally for a period of 1 year, from specific requirements imposed by this Order, pending completion of actions which will result in conformance with the requirements. Interim compensatory security measures are required.

bg. Working Papers. Documents and material accumulated or created while preparing finished material (e.g., classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents).

Appendix C

Guidelines for a Command Security Instruction/Turnover Binder

1. The security manager shall assess the vulnerability of the command's classified NSI to loss or compromise. This includes obtaining information on the local threat, volume and scope of classified NSI, mission of the command, countermeasures available and the cost and effectiveness of alternative courses of action.

a. Results of this assessment shall be used to develop a command security instruction which shall mirror the organization of this regulation and identify any unique command requirements.

b. The command security instruction shall supplement this regulation and other directives from authorities in the command administrative and operational chain.

2. Incorporate the following into the command security instruction:

a. The purpose, applicability, and relationship to other directives, particularly this regulation.

b. Identify the chain of command.

c. Describe the security organization and identify positions.

d. Define the responsibilities of the Command Security Manager and SSO if applicable.

e. Cite and append SSA's, if applicable.

f. Describe procedures for internal and subordinate security reviews and inspections.

g. Specify internal procedures for reporting and investigating loss, compromise, and other security discrepancies.

h. Establish procedures to report CI matters to the responsible Marine Corps CI office for the unit to coordinate with NCIS. If there is no responsible Marine Corps CI office, forward to the nearest NCIS office for disposition.

30 JAN 2017

- i. Develop an IPSP security education program. Assign responsibilities for briefings and debriefings.
- j. State whether the Commanding Officer and any other command officials have been delegated Top Secret or Secret original classification authority.
- k. Establish procedures for the review of classified NSI prepared in the command to ensure correct classification and marking. Identify the sources of security classification guidance commonly used, and where they are located.
- l. Develop an Industrial Security Program and identify key personnel, such as the COSR, if applicable. The Industrial Security Program should include regular coordination between the COSR, Command Security Manager, IAM and contractor point of contact to ensure that all security procedures are being followed to include IT designations, investigations and eligibility requirements.
- m. Specify command responsibilities and controls on any special types of classified and controlled unclassified NSI.
- n. Establish reproduction controls to include compliance with reproduction limitations and any special controls placed on information by originators.
- o. Identify requirements for the safeguarding of classified NSI. This includes, but is not limited to, the following: how classified NSI shall be protected during working hours, storage requirements, transported in and out of the command and while in a travel status; and the conduct of classified meetings. The safeguarding of classified NSI located in foreign countries, IT processing equipment and residential storage arrangements are additional considerations.
- p. Establish command destruction procedures. Identify destruction facilities or equipment available. Attach a command emergency destruction plan, as a supplement, when required.
- q. Establish command visitor control procedures to accommodate visits to the command involving access to, or disclosure of, classified NSI. Identify procedures to include verification of personnel security clearances and Need-to-Know.

30 JAN 2017

3. A turnover binder shall be maintained in addition to the Command Security Instruction. This binder shall include, but is not limited to, the following information:

a. Points of contact. This should include but is not limited to: Provost Marshall Office, local NCIS field office, PAO, COR, IAM, FDO, GSA approved locksmith, command section leadership, adjudication facility help desk, etc.

b. Daily, weekly, monthly and annual procedures and requirements. This includes internal and external reports. The JPAS Personnel and Periodic Reinvestigation reports should be no more than 30 days old.

c. Maintain current copies of T/O and TOECR submissions.

d. Command inventory of classified material and locations.

e. List of contractors working within the command along with visit requests for each.

f. Access rosters for the command.

g. Appointment letters for all security related billets.

h. Identify the security manager chain of command up to the MARFOR level.

i. Identify the SOI, SON, SMO code, and e-QIP agency ID.

j. Command Security Instruction.

k. List of all in command with Temporary Access along with Commander's justification letter, if appropriate.

l. Suspense roster for all pending security actions, i.e., initiated PSIs, open investigations, LOIs, contractor VRs.

m. Templates to include, but not limited to, appointment letters, Continuous Evaluation Report, PIPS Form 12, OPM Portal request, etc.

n. e-QIP users guide, training materials, command specific instructions.

30 JAN 2017

o. Identify security training resources for the command, including security personnel. Resources include online training, HQMC IPSP SharePoint, and command specific training.

p. List of all security containers and restricted areas along with locations and appropriate Physical Security Surveys.

Appendix D

Emergency Plan and Emergency Destruction Supplement

Part One: Emergency Action Plan (EAP)

1. Commanding Officers shall develop an EAP for the protection of classified NSI in case of a natural disaster or civil disturbance. The EAP may be prepared in conjunction with the command's disaster preparedness plan.
2. EAPs provide for the protection of classified NSI in a way that shall minimize the risk of personal injury or loss of life. For instance, plans should call for immediate personnel evacuation in the case of a fire, and not require that all classified NSI be properly stored prior to evacuation. A perimeter guard or some mechanism to control access to the area shall provide sufficient protection without endangering personnel.
3. In developing an EAP, assess the command's risk posture. Consider the size and composition of the command; the amount of classified NSI held; situations which could result in the loss or compromise of classified NSI; the existing physical security measures; the location of the command and degree of control the Commanding Officer exercises over security (e.g., a ship versus a leased private building); and local conditions which could erupt into emergency situations.
4. Once a command's risk posture has been assessed, it can be used to develop an emergency plan which can take advantage of a command's security strengths and better compensate for security weaknesses. At a minimum, the emergency plan shall designate persons authorized to:
 - a. Decide that an emergency situation exists and to implement emergency plans.
 - b. Determine the most effective use of security personnel and equipment.
 - c. Coordinate with local civilian law enforcement agencies and other nearby military commands for support.
 - d. Consider transferring classified NSI to more secure storage areas in the command.

30 JAN 2017

- e. Designate alternative safe storage areas outside the command.
- f. Identify evacuation routes and destinations.
- g. Arrange for packaging supplies and moving equipment.
- h. Educate command personnel in emergency procedures.
- i. Give security personnel and augmenting forces additional instruction on the emergency plan.
- j. Establish procedures for prompt notification of appropriate authorities in the chain of command.
- k. Establish the requirement to assess the integrity of the classified NSI after the emergency.

Part Two: Emergency Destruction Supplement

1. Commands located outside the U.S. and its territories and units that are deployable, require an emergency destruction supplement for their EAP (EKMS policy documents provide additional emergency destruction policy and guidance for commands that handle COMSEC equipment and information).
 - a. Conduct emergency destruction drills as necessary to ensure that personnel are familiar with the plan and associated equipment.
 - b. Any instances of incidents or emergency destruction of classified NSI shall be reported to PS.
2. The priorities for emergency destruction are:
 - a. Priority One - Top Secret information.
 - b. Priority Two - Secret information.
 - c. Priority Three - Confidential information.
3. For effective emergency destruction planning, limit the amount of classified NSI held at the command and if possible store less frequently used classified NSI at a more secure command.

30 JAN 2017

a. Consideration shall be given to the transfer of the information to electronic media, which shall reduce the volume needed to be transferred or destroyed.

b. Should emergency destruction be required, any reasonable means of ensuring that classified NSI cannot be reconstructed is authorized.

4. An emergency destruction supplement shall be practical and consider the volume, level, and sensitivity of the classified NSI held at the command; the degree of defense the command and readily available supporting forces can provide; and proximity to hostile or potentially hostile countries and environments.

a. More specifically, the emergency destruction supplement shall delineate the procedures, methods (e.g., document shredders or weighted bags), and location of destruction; indicate the location of classified NSI and priorities for destruction; identify personnel responsible for initiating and conducting destruction; authorize the individuals supervising the destruction to deviate from established plans if warranted; and emphasize the importance of beginning destruction in time to preclude loss or compromise of classified NSI.

b. The command must ensure that the means are available within the command to execute emergency destruction without necessitating outside intervention (e.g., tools for manual destruction of documents/material via burning and smashing of classified electronic devices) must be available.

5. Marine Corps commands and organizations aboard Naval vessels shall ensure that they became familiar with the emergency destruction procedures in place aboard ship. Coordination must be effected to include Marine Corps classified material in the destruction plan.

Appendix E

Commander's Checklist for Granting Access

1. These instructions were developed to assist the commander in ensuring that only those personnel who are properly cleared possess access to classified NSI within the command. Any questions arising which are not covered by these instructions may be answered with a review of SECNAV M-5510.30.

2. Commander's Actions:

a. Determine the level of access required by the Marine/civilian.

b. Determine eligibility assigned by viewing JPAS records.

c. If the Marine/civilian possesses appropriate eligibility, ensure the following:

(1) Confirm U.S. citizenship.

(2) Review Marine's SRB/OQR, PMO records, SACO reports, APC credit card delinquency reports, health/dental records, and any other locally available records for any potentially disqualifying information which could adversely affect eligibility. If information of this nature is discovered, it will be reported via the incident report link in JPAS and reviewed locally to determine whether the risk is too great to assign access to classified NSI.

(3) If warranted, assign access no higher than established eligibility and 'Need-to-Know' based solely on billet requirements.

(4) Record individual on unit access roster and in JPAS.

d. If Marine/civilian does not possess appropriate eligibility, ensure the following:

(1) Confirm U.S. citizenship.

(2) Review records as indicated in Paragraph 1.c.(2) above.

30 JAN 2017

(3) Review SECNAV M-5510.30 to determine investigative requirement.

(4) Submit request for appropriate PSI.

(5) Assign access or temporary access per the provisions of Reference (u). If potentially disqualifying information is reported in the SF 86 or local records, Temporary Access decisions will include a written endorsement from the CO. This endorsement will Reference any information that could be considered derogatory along with a risk management decision which considers derogatory information and potential mitigating factors. A recommended format for this letter is at Appendix E.

(6) Assign collateral temporary access as allowed by reference (j).

(7) Record individual on unit access roster and in JPAS.

Appendix F

Temporary Access Authorization Letter Format

ORGANIZATIONAL
LETTERHEAD

5520
Section ID
Date

MEMORANDUM

From: Commanding Officer
To: Files

Subj: TEMPORARY ACCESS AUTHORIZATION LETTER FOR (INSERT RANK
AND NAME)

Ref: (a) SECNAV M-5510.30
(b) MCO 5510.18B

1. I have determined that it is in the best interest of the national security and the mission of this command that (Insert Rank and Name) be granted Temporary Access at the level of (insert level of access).

2. A review of the SF86 and other available records indicates the presence of the following potentially disqualifying information:

a.

b.

3. The Command Security Manager will ensure that the following steps are taken to mitigate the risk associated with this decision:

a.

b.

4. The point of contact for this issue is (Rank and Name), Command Security Manager at (phone number and email address).

I.M. MARINE
Rank

Appendix G

Classified Material Control Center

1. The term CMCC is not defined in other policy documents though it is typically understood to mean a location through which a command controls classified documents and material. It may be as elaborate as a vault with multiple security specialists to a two drawer GSA approved security container in a corner of an office. Regardless of the size or scope of a command's classified holdings, the term CMCC describes the place from which classified holdings are centrally controlled.

2. The CMCC should be managed by the Command Security Manager. There are no restrictions on "ownership" of the CMCC and there is no conflict of interest in having the Command Security Manager in charge of the CMCC. In fact, there are many positive aspects associated with having the subject matter expert charged with the management of the command's classified holdings.

3. This appendix provides an example of how to establish and manage a CMCC. This is not directive in nature but provides a place to start. The CMCC is effective if it can identify all items of classified material within the command, where it's located and when it's destroyed.

4. Control of Secret documents need not be complicated. A simple logbook or spreadsheet with locally generated control numbers for the documents is sufficient. The following is an example of how this might be achieved.

a. Document Control Number. The control number may be any number that uniquely identifies the document within the command. The example below consists of the unit RUC, Julian Date and Document Number to read as follows:

Command's RUC	54008
Julian Date Created or entered command	9236
Container Number	Letter or Number (A or 3)
Document Number	01

Example final number would read: 54008-9236-A-01

The Julian Date is recommended as a simplified manner to enter the date. Rather than attempting to use, 090824 or 24Aug09, the four digit Julian Date is constructed such that the Julian day

30 JAN 2017

as shown in Tables T-1 and T-2. Of course, it requires the maintenance of a Julian Date calendar to decipher the number. As stated earlier, this is merely an example.

b. Document Control Spreadsheet. The spreadsheet below is simply an example of how this might be done. Separate spreadsheets can be placed in each container to allow the person logging it into the Command to complete the log. Periodically, the spreadsheet could be entered into a computer based database to reduce the need for maintenance of paper logs.

SAMPLE DOCUMENT INVENTORY SHEET

Subject	Docume nt Date	Classificati on	Docume nt Contro l Number	Dispositi on	Name/Signatu re of person taking action
Widgets required for MEU Deployme nt	18 May 09	SECRET	54008- 9236- A-01	Destroyed 9249	Butler, S.
OPORD 3- 08	4 Mar 08	SECRET	34708- 8064- B-03	Transferr ed to HQMC	Lejeune, J.
Hard Drive		SECRET	54008- 7245- A-06		

Maintaining one spreadsheet per security container allows subsequent document numbers to simply continue with the next number. Documents in different containers are differentiated by separate container numbers. Commands with the same RUC but many different staff agencies with multiple Secondary Control Points (SCP) can simply use a separate command identifier. For example, Headquarters, Marine Corps can use the commonly known Department, Division and Branch identifiers. A document controlled by Security Division of Plans, Policies and Operations, controlled on 24 Aug 2009, in container A, document number 01 would appear like, PS-9236-A-01.

30 JAN 2017

TABLE-1
 JULIAN DATE CALENDAR
 (PERPETUAL-NON LEAP YEARS)

DAY	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	DAY
1	001	032	060	091	121	152	182	213	244	274	305	335	1
2	002	033	061	092	122	153	183	214	245	275	306	336	2
3	003	034	062	093	123	154	184	215	246	276	307	337	3
4	004	035	063	094	124	155	185	216	247	277	308	338	4
5	005	036	064	095	125	156	186	217	248	278	309	339	5
6	006	037	065	096	126	157	187	218	249	279	310	340	6
7	007	038	066	097	127	158	188	219	250	280	311	341	7
8	008	039	067	098	128	159	189	220	251	281	312	342	8
9	009	040	068	099	129	160	190	221	252	282	313	343	9
10	010	041	069	100	130	161	191	222	253	283	314	344	10
11	011	042	070	101	131	162	192	223	254	284	315	345	11
12	012	043	071	102	132	163	193	224	255	285	316	346	12
13	013	044	072	103	133	164	194	225	256	286	317	347	13
14	014	045	073	104	134	165	195	226	257	287	318	348	14
15	015	046	074	105	135	166	196	227	258	288	319	349	15
16	016	047	075	106	136	167	197	228	259	289	320	350	16
17	017	048	076	107	137	168	198	229	260	290	321	351	17
18	018	049	077	108	138	169	199	230	261	291	322	352	18
19	019	050	078	109	139	170	200	231	262	292	323	353	19
20	020	051	079	110	140	171	201	232	263	293	324	354	20
21	021	052	080	111	141	172	202	233	264	294	325	355	21
22	022	053	081	112	142	173	203	234	265	295	326	356	22
23	023	054	082	113	143	174	204	235	266	296	327	357	23
24	024	055	083	114	144	175	205	236	267	297	328	358	24
25	025	056	084	115	145	176	206	237	268	298	329	359	25
26	026	057	085	116	146	177	207	238	269	299	330	360	26
27	027	058	086	117	147	178	208	239	270	300	331	361	27
28	028	059	087	118	148	179	209	240	271	301	332	362	28
29	029		088	119	149	180	210	241	272	302	333	363	29
30	030		089	120	150	181	211	242	273	303	334	364	30
31	031		090		151		212	243		304		365	31

30 JAN 2017

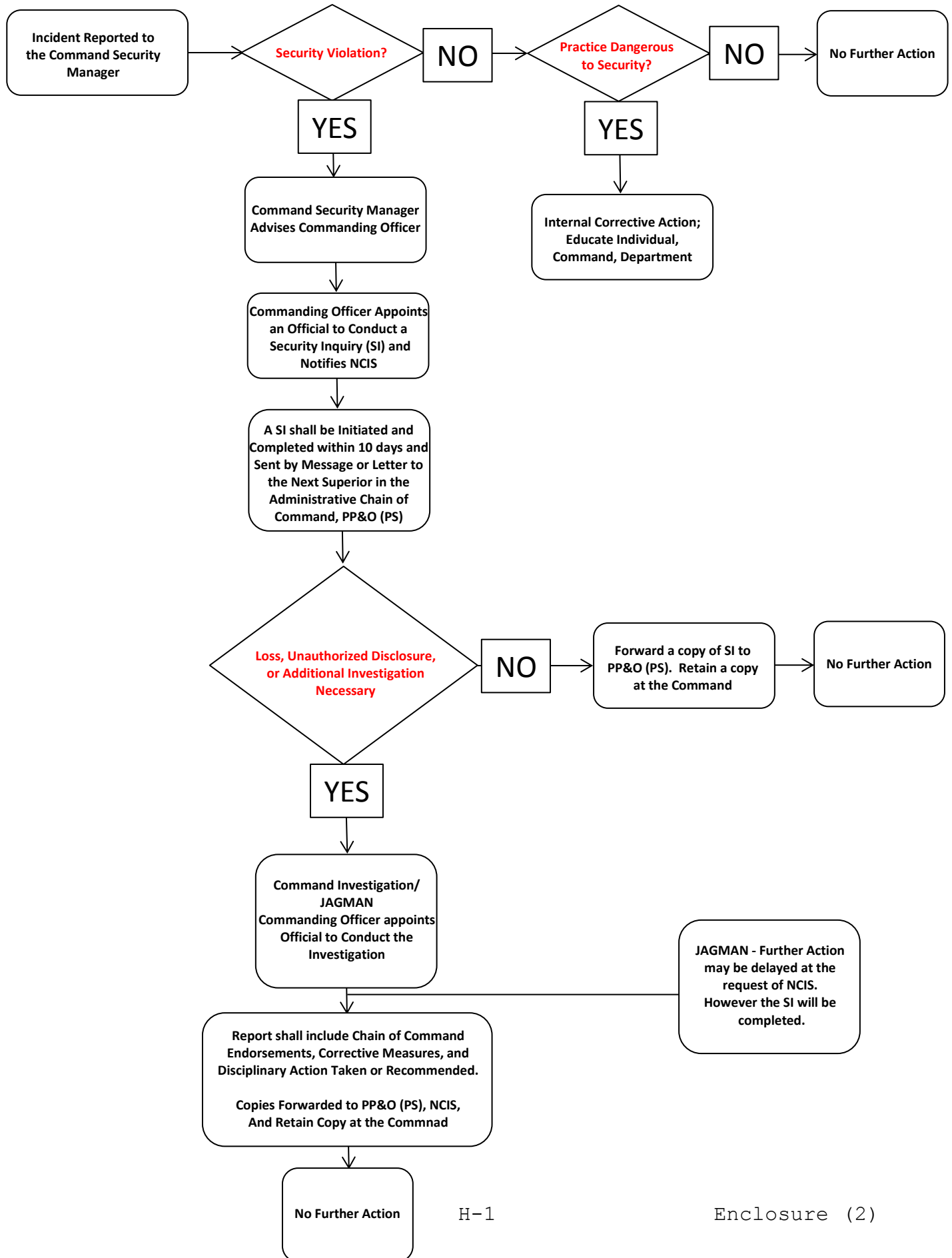
TABLE-2
 JULIAN DATE CALENDAR
 (FOR LEAP YEARS ONLY)

DAY	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	DAY
1	001	032	061	092	122	153	183	214	245	275	306	336	1
2	002	033	062	093	123	154	184	215	246	276	307	337	2
3	003	034	063	094	124	155	185	216	247	277	308	338	3
4	004	035	064	095	125	156	186	217	248	278	309	339	4
5	005	036	065	096	126	157	187	218	249	279	310	340	5
6	006	037	066	097	127	158	188	219	250	280	311	341	6
7	007	038	067	098	128	159	189	220	251	281	312	342	7
8	008	039	068	099	129	160	190	221	252	282	313	343	8
9	009	040	069	100	130	161	191	222	253	283	314	344	9
10	010	041	070	101	131	162	192	223	254	284	315	345	10
11	011	042	071	102	132	163	193	224	255	285	316	346	11
12	012	043	072	103	133	164	194	225	256	286	317	347	12
13	013	044	073	104	134	165	195	226	257	287	318	348	13
14	014	045	074	105	135	166	196	227	258	288	319	349	14
15	015	046	075	106	136	167	197	228	259	289	320	350	15
16	016	047	076	107	137	168	198	229	260	290	321	351	16
17	017	048	077	108	138	169	199	230	261	291	322	352	17
18	018	049	078	109	139	170	200	231	262	292	323	353	18
19	019	050	079	110	140	171	201	232	263	293	324	354	19
20	020	051	080	111	141	172	202	233	264	294	325	355	20
21	021	052	081	112	142	173	203	234	265	295	326	356	21
22	022	053	082	113	143	174	204	235	266	296	327	357	22
23	023	054	083	114	144	175	205	236	267	297	328	358	23
24	024	055	084	115	145	176	206	237	268	298	329	359	24
25	025	056	085	116	146	177	207	238	269	299	330	360	25
26	026	057	086	117	147	178	208	239	270	300	331	361	26
27	027	058	087	118	148	179	209	240	271	301	332	362	27
28	028	059	088	119	149	180	210	241	272	302	333	363	28
29	029	060	089	120	150	181	211	242	273	303	334	364	29
30	030		090	121	151	182	212	243	274	304	335	365	30
31	031		091		152		213	244		305		366	31

(USE IN 2004, 2008, 2012, 2016, ETC)

Appendix H
COLLATERAL SECURITY INCIDENT FLOWCHART

MCO 5510.18B
 30 JAN 2017



Appendix I

PRIVACY ACT STATEMENT

In accordance with the Privacy Act of 1974 (Public Law 93-579), this notice informs you of the purpose for collection of information on this form. Please read it before completing the form.

AUTHORITY: 5 U.S.C. 9101, Access to Criminal History Information for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; DoD Directive 1145.02E, United States Military Entrance Processing Command (USMEPCOM); DoD 5200.2R, DoD Personnel Security Program (PSP); DoD 5105.21, Sensitive Compartment Information Administrative Security Manual; DoD Instruction (DoDI) 1304.26, Qualification Standards for Enlistment, Appointment and Induction; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE: Information collected by this form will be used to determine the official status of your most recent personnel security investigation, employment suitability investigation, any determinations regarding assignment of eligibility for access to classified National Security Information. The information collected on this form will be filed within a Privacy Act Systems of Records collection governed by Privacy Act System of Records Notice (PA SORN) DMDC 12 DoD available at <http://dpcl.d.defense.gov/Privacy/SORNSIndex/DOD-wide-SORN-Article-View/Article/570567/dmdc-12-dod/>

ROUTINE USES: Records may be accessed by authorized security personnel with a Need-to-Know to confirm an individual's authorized access to classified information.

DISCLOSURE: Providing information on this form is mandatory for military personnel and voluntary for civilian and contractor personnel. Note that failure to provide the requested information will result in a denial of classified access.