UNITED STATES MARINE CORPS
MARINE CORPS RECRUIT DEPOT/EASTERN RECRUITING REGION
PO BOX 19001
PARRIS ISLAND, SOUTH CAROLINA 29905-9001

DepO 5510.14A
G-3
14 MAY 2010

DEPOT ORDER 5510.14A

From: Commanding General
To: Distribution List

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.30B
(b) SECNAVINST 5510.36A
(c) MCO P5510.18A
(d) National Industrial Security Program Operating Manual
(e) MARADMIN 624/08
(f) Depot Order 5500.9G
(g) MARADMIN 0066/09
(h) Depot Order 1601.1B
(i) Marine Corps Enterprise IA Dir 011 PII

Encl: (1) Introduction to the Information and Personnel Security Program
(2) Personnel Security Investigations, Determinations, and Clearances
(3) Continuous Evaluation Program
(4) Security Education
(5) Access to Classified Information
(6) Industrial Security Program

1. Situation. To disseminate policies and procedures for the effective management, operation, and maintenance of Marine Corps Recruit Depot (MCRD) Eastern Recruiting Region (ERR) and Parris Island (PI) Information and Personnel Security Program pursuant to the guidelines established in references (a) through (i).

2. Cancellation. DepO P5510.14.

3. Mission. To provide uniformity and effectiveness in the application of the Information and Personnel Security Program for the MCRD/ERR PI.

4. Execution. The MCRD/ERR PI Information and Personnel Security Program is established in compliance with the Department of the Navy (DON) Security Program. The program ensures information and personnel security management responsibilities are fulfilled to include the responsibility of the Commanding General and AC/S G-3 to safeguard all classified information within this command. Enclosures (1) through (6) encompass each section of the Information and Personnel Security Program. Recommendations to this order are invited and should be submitted to the Command Security Manager via the appropriate chain of command.

5. Administration and Logistics. This order establishes coordinated policies for maintenance of the Information and Personnel Security Program it is applicable to all organizations and activities stationed aboard the MCRD/ERR PI.

6. Command and Signal

a. Command. This order is applicable to all personnel aboard MCRD PI and within ERR.

b. Signal. This order is effective the date signed

R. L. GRABOWSKI
Chief of Staff

DISTRIBUTION: A

Introduction to the Information and Personnel Security Program

1. Basic Policy. The MCRD/ERR PI Information and Personnel Security Program is established in compliance with the references.

2. Authority

a. The Commanding General, MCRD/ERR PI is responsible for establishing and maintaining an Information and Personnel Security Program in compliance with the references.

b. The Command Security Manager is the principal advisor on information and personnel security and is responsible to the Commanding General for the security program management.

c. The responsibility for the security and proper handling of classified material extends directly to the individual having knowledge or possession of such material and to activity heads within whose purview classified material is utilized.

d. Individual requests for guidance or interpretation of this order should be addressed to the Command Security Manager.

3. Applicability

a. This order establishes coordinated policies for the protection of classified information and for personnel security matters by incorporating the policies of numerous DoD/DON/USMC directives.

b. As this order establishes coordinated policies for maintenance of the Information and Personnel Security Program it is applicable to all activities at the MCRD/ERR PI.

4. Responsibility for Compliance

a. The Command Security Manager is responsible for compliance with and implementation of this order for all activities at the MCRD/ERR PI.

b. Commanding Officers and department activity heads are responsible for compliance with and implementation of this order within their activity.

c. All Navy and Marine Corps personnel are responsible for compliance with this order in all respects.

d. All activities that hold, handle or otherwise come in contact with classified information will at a minimum have on hand and maintain the references and this order.

5. Program Management

a. The Command Security Manager manages the Information and Personnel Security Program for the MCRD/ERR PI. The Command Security Manager is responsible for all information and personnel security matters for each

subordinate unit and District to include all military and DON/USMC civilian personnel assigned to the MCRD/ERR PI.

b. The following appointments by the Commanding General (CG) will be made in writing, setting forth the requirements that they be familiar with the specific portions of the references. The appointment letters shall be forwarded to CNO N09N2 and HQMC PP&O/PS for record:

(1) Security Managers and other security personnel will obtain formal training within 90 days of appointment. The Security Manager's Course is offered by an MTT from HQMC PP&O/PS. This course will provide Marine Corps-specific information and discuss the day-to-day mechanics of managing a Marine Corps command's security program. The HQMC Security Manager's Training Course will be the first choice before sending Marines to the course offered by the Naval Criminal Investigative Service (NCIS) Security Training and Assistance Team (STAAT). Either MTT will satisfy basic security management training requirements. Additional information may be found on the Navy Security website at CNO WEB URL http://www.navysecurity.navy.mil/.

(2) Each command will prepare and maintain a written command security instruction, specifying how security procedures and requirements will be accomplished in the command.

(3) Command Security Manager

(a) Commands in the Marine Corps eligible to receive classified information, generally all Squadron/Battalion level commands and above, are required to designate a Command Security Manager, in writing. The presence of a Command Security Manager goes well beyond the management of classified information/material as it also supports the personnel security program. Commands which do not have a Command Security Manager must be a participant in a Security Servicing Agreement with another command which has agreed to provide Information and Personnel Security services.

(b) The Command Security Manager will, at a minimum, be considered a Special Staff Officer and will be afforded direct access to the Commanding Officer to ensure effective management of the command's information and personnel security program. This access will not be subjected to prior screening. The Command Security Manager must be provided sufficient authority and staff to manage the program for the command.

(c) The Command Security Manager will be assigned per references (a) and (c). The Command Security Manager may not be a contractor.

(4) Command 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. The designation must be in writing. Assistant Security Managers must have an SSBI only if they are designated by the command to authorize Temporary Access (formerly Interim Clearance); otherwise, the investigative and eligibility requirements will be determined by the level of access to classified information required.

6. Duties of the Command Security Manager

a. The duties of the Command Security Manager are delineated in references (a) and (c). The Command Security Manager is the principal advisor to the Commanding General on the Information and Personnel Security Program (IPSP) and is responsible to the Commanding General for the management of the program. The duties described in this Order may apply to a number of personnel. 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. 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. The Command Security Manager plays a critical role in developing and administering the command's Information and Personnel Security Program (IPSP).

b. The duties listed below apply to the Command Security Manager:

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

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

(3) Develops written command information and personnel security procedures, including an emergency plan which integrates emergency destruction plans where required.

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

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

(6) Ensures that all personnel who will handle classified information or will be assigned to sensitive duties are appropriately cleared through coordination with the Department of the Navy Central Adjudication Facility (DON CAF) and that requests for personnel security investigations are properly prepared, submitted and monitored.

(7) Ensures that access to classified information is limited to those who are eligible and have a verifiable need-to-know.

(8) Ensures that personnel security investigations, clearances and accesses are properly recorded within the Joint Personnel Adjudication System (JPAS).

(9) Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

(10) If applicable, maintains liaison with the Command Special Security Officer (SSO) concerning information and personnel security policies and procedures.

(11) Coordinates with the command Information Assurance Manager (IAM) on matters of common concern.

(12) Ensures that all personnel who have had access to classified information who are separating, retiring or relieved for cause per reference (b) have completed a Security Termination Statement. The Security Termination Statement must then be forwarded to HQMC M&RA (MMSB-20) for inclusion in the OMPF. The address is found in reference (a).

(13) Ensures all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information. Hard copy SF 312's will be forwarded to HQMC (MMSB-20), with the execution documented within JPAS.

7. Other Security Assistants. The Information and Personnel Security Program establishes a network of personnel throughout the Command to implement the program to include effective security, control, and utilization of classified material.

a. 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 they have the appropriate eligibility necessary for the access or position sensitivity required to perform their assigned duties and tasking.

b. Information Assurance Manager (IAM). Each command involved in processing data in an automated system, including access to local area networks and/or INTRANET/INTERNET, must designate a civilian or military member as an IAM. The IAM is responsible for development, maintenance, and implementation of the INFOSEC program within the activity. The IAM advises on all INFOSEC matters, including identifying the need for additional INFOSEC staff. The IAM serves as the command's point of contact for all INFOSEC matters and implements the command's INFOSEC program. The Marine Corps Information Assurance web site at https://hqdod.hqmc.usmc.mil/IA.asp provides further guidance.

c. Contracting Officer's Representative (COR). Commands which award contracts to industry requiring access to classified information by the contractor and employees or which will result in the development of classified information and/or equipment will appoint, in writing, one or more qualified specialists as Contracting Officer's Representatives (COR). Details concerning COR responsibilities and requirements are contained in Enclosure 6 of this order.

d. The Commanding Officer of each subordinate unit will appoint a security liaison for the Command Security Manager for information and personnel security matters. The Commanding Officer may appoint an additional security liaison if deemed necessary. The appointed liaison shall inform the Command Security Manager of all security violations and/or related information and personnel security issues.

10. Inspections and Review

a. The Commanding General is responsible for the evaluation of the effectiveness of the Information and Personnel Security Program for the Command.

b. Qualified personnel will conduct inspections, assist visits, and reviews to examine the command's overall information and personnel security posture.

c. The Command Security Manager is the section to be inspected for all subordinate units and Districts.

d. An annual assist visit will be conducted for the Command program.

e. The Command Security Manager will conduct annual self-inspections of the program.

f. A command information and personnel security program self-inspection guide is provided in references (a) and (b). These checklists may be modified to meet local command needs. The Inspector General of the Marine Corps (IGMC) Security Inspection checklist (FA 270) may be found in the Automated Inspection Reporting System (AIRS) available on the IGMC page at, http://hqinet001.hqmc.usmc.mil/ig/Div_Inspections/AIRS%20CHECKLIST/AIRS_Index.htm. The AIRS Checklist will be used for all inspections initiated by HQMC. However, the checklist is only a point of departure. Any area within the command subject to a requirement established by any reference in this order is subject to inspection.

g. Unannounced security inspections may be conducted periodically by security management personnel to ensure secure posture is effective.

7. Emergency Plans

a. The Command will maintain Reference (f), the emergency plan for the protection of classified material and communications security material (COMSEC) in case of natural disaster, civil disturbance, or an attempt by an individual(s) to compromise classified information. This plan must be detailed with specific procedures and responsibilities.

b. In developing emergency plans, the guidance contained in reference (b) will be utilized.

c. References (f) and (b) shall be utilized in the case of natural disaster, civil disturbance, or an attempts by an individual(s) to compromise classified information.

Personnel Security Investigations, Determinations, and Clearances

1. Basic Policy. Guidance concerning personnel security investigations (PSI), clearance eligibility determinations, and clearance access is contained in reference (a).

2. Personnel Security Investigations. Required PSI requests for ERR and Depot personnel will be processed via the Command Security Manager.

3. Clearance Eligibility Determinations

a. The term "security clearance eligibility" has replaced "security clearance," when referring to a formal security determination made by an authorized adjudicative facility.

b. The Department of the Navy Central Adjudication Facility (DoNCAF) will correspond with the Office of the Command Security Manager regarding any adjudication issues which include, but are not limited to, Letters of Intent (LOI) to Deny or Revoke, CAF messages, and Letters of Notification (LON).

(1) Subordinate units must forward mail correspondence received directly by DoNCAF to the Command Security Manager for action.

(2) Responses to Letters of Intent to Deny or Revoke and appeals to Letters of Notification will be coordinated through the Command Security Manager. The Command Security Manager acts as the single point of contact for due process and appeals.

(3) The Command Security Manager will coordinate the process via the individual's commanding officer at the battalion or district level. The individual's commanding officer must endorse the individual's response to the LOI and/or LON.

(4) Per reference (c), all PCS and PCA orders must be cancelled or held in abeyance pending the final outcome of due process.

4. Clearance Access

a. Clearance access to classified information is granted by the Command in accordance with reference (a). The Command Security Manager ensures that access to classified information is limited to those who are eligible and have a verifiable need-to-know. Access is not based on rank, position, or only clearance eligibility. It is based on need-to-know and established security clearance eligibility.

b. A Classified Information Nondisclosure Agreement (SF 312) will be executed by all persons requesting access.

c. Security Termination Statement will be executed by all persons being de-briefed from access to classified information.

d. The Office of the Command Security Manager shall ensure appropriate procedures are followed regarding access to classified information.

e. Temporary collateral clearances are granted by the Command in accordance with reference (a).

5. Joint Personnel Adjudication System (JPAS)

a. The Joint Personnel Adjudication System (JPAS) is the system of record to be used to manage PSIs, clearance eligibility, communication with DoNCAF, access to classified information, and overall personnel and information security management.

b. Printouts of JPAS personnel summary screens are authorized for distribution for clearance eligibility verification. Verification letters may also be issued for personnel requiring verification of clearance eligibility.

c. The Command Security Manager shall maintain the Personnel Management Net (PSMNet) via JPAS.

Continuous Evaluation Program

1. Basic Policy. Refer to reference (a) for guidance regarding the Continuous Evaluation Program.

2. Continuous Evaluation Program

a. Per reference (a), the Continuous Evaluation Program must be implemented in order to ensure that individuals who have been granted security clearance eligibility remain eligible through continuous assessment and evaluation. Commands must report any questionable or unfavorable information concerning an individual with security clearance eligibility.

b. Exhibit 10A of reference (a) states that the following security issues must be reported to DoNCAF:

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

(2) Foreign influence concerns/close personal association with foreign nationals or nations.

(3) Foreign citizenship (dual citizenship) or foreign monetary interests.

(4) Sexual behavior that is criminal or reflects a lack of judgment or discretion.

(5) Conduct involving questionable judgment, trustworthiness, unreliability or unwillingness to comply with rules and regulations, or unwillingness to cooperate with security clearance processing.

(6) Excessive indebtedness or unexplained affluence.

(7) Alcohol abuse.

(8) Illegal or improper drug use/involvement.

(9) Apparent mental, emotional or personality disorder(s).

(10) Criminal conduct.

(11) Noncompliance with security requirements.

(12) Engagement in outside activities that could cause a conflict of interest.

(13) Misuse of Information Technology Systems.

c. Reports of questionable or unfavorable information shall be reported to the Office of the Command Security Manager at the time the information becomes available. Reports will then be submitted to DoNCAF via JPAS.

d. The Command Security Office should have access to a variety of sources containing reportable information. Examples of sources are Relief for Cause (RFC) packages, military police blotters, and the Officer Discipline Notebook (ODN).

e. The command's report of derogatory information does not automatically revoke an individual's security clearance eligibility. DoNCAF will properly evaluate the command report and the adjudication will be posted in JPAS.

f. Per reference (c), all PCS and PCA orders must be cancelled or held in abeyance pending the final outcome of the incident report.

Security Education

1. Basic Policy. Security briefing requirements are contained in Chapter 4 of reference (a).

2. Types of Briefings. The Command Security Manager will ensure that the following briefings are conducted:

a. Orientation Briefing. Military and civilian personnel with security clearance eligibility will receive a security orientation upon reporting aboard or being assigned to sensitive IT duties or duties involving access to classified information.

b. Initial Security Brief. An initial security brief will be given to all individuals when they are granted access to classified information.

c. Command Debriefing. Individuals no longer requiring access to classified information on those occasions listed in the SECNAV 5510.30 will be given a command debriefing. A Security Termination Statement is an additional element of the command debriefing and must be completed by all personnel no longer requiring access to classified information. Individuals transferring to a command where access will be continued are not required to complete the Security Termination Statement.

d. On-the-Job Training. Supervisors and leaders will provide on-the-job training to ensure subordinates know the security requirements impacting their duties. Aspects of training include, but are not limited to, the proper use of SF 701, local access procedures for the work area, protecting sensitive unclassified material, and safeguarding classified information.

e. Annual Refresher Briefing. Personnel with security clearance eligibility will be given an annual refresher briefing. In most cases, the Commanding Officer, supervisor, training officer, or other designated organization or activity point of contact will ensure all personnel have completed the training per the guidance from the Command Security Manager. The Office of the Command Security Manager will maintain a record of all annual training received.

f. Counter-Intelligence. All personnel who have access to Secret and above shall receive annual briefings on all threats posed by foreign intelligence and terrorist organizations.

g. Foreign Travel Briefing. A foreign travel briefing is required for all personnel with access to classified information who travel to a foreign country. Upon request, an unclassified version of the briefing may be given to those without access to classified information.

h. NATO Briefing. NATO briefings will be conducted for all USMC personnel who have access to SIPRNET per MARADMIN 136/04.

2. Security Awareness. The security education program will include continuous and frequent exposure to current information and other awareness materials. Signs, posters, intranet webpage postings, email notifications,

and Security Manager's Notes are examples of media that should be used to promote security awareness.

3. Security Training Requirements. Specific job training is required for incumbents in the following designated positions: security manager, security specialist, classified courier, and personnel assigned to DON IT positions.

Access to Classified Information

1. Basic Policy. References (a) and (b) establish the minimum standards for accessing, classifying, safeguarding, transmitting, disseminating and destroying classified information as required by a higher authority. Reference (b) shall be utilized for all Information Security Program (ISP) matters for the ERR and Depot.

2. Visitor Access to Classified Information

a. Only visitors with an appropriate level of security clearance and need to know are granted access to classified information. If an escort is required for the visitor, a properly trained military or civilian member assigned to the Command may be used. The activity receiving the visitor is responsible for ensuring that the visitor has proper identification. Report any attempt to gain access to classified information by persons using fraudulent IDs to the Command Security Manager and the Naval Criminal Investigative Service (NCIS).

b. The term visitor applies to any person who is not attached to or employed by MCRD/ERR PI. A person on temporary additional duty is also considered a visitor.

c. The Command Security Manager maintains a military, civilian, and contractor visitor access roster.

3. Visit Request. All visit requests to or from ERR/MCRD Parris Island will be forwarded via JPAS.

4. Foreign Visits

a. Reference (a and b) provide guidance on foreign nationals and representatives of foreign entities disclosure of classified information to foreign governments.

b. Foreign visits are handled through the G-3 (Operations Division).

c. The designated Foreign Disclosure Office must be contacted in advance regarding foreign visits and potential disclosure of classified information.

5. Storage and Destruction

a. Refer to Chapter 10 of reference (b) for complete guidance regarding storage requirements for classified information.

b. The Commanding General is responsible for safeguarding all classified information within this command. The G-3 has staff cognizance for this function and will ensure that it is stored as prescribed in reference (b).

c. Only approved, designated containers will be used for storage of classified material.

d. The General Services Administration (GSA) established and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, and associated security devices suitable for the storage and destruction of classified information. These are available at the DoD Lock Program Site: https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks.

e. Report any weakness or deficiency in equipment being used to safeguard classified material in storage to the Command Security Manager. Reports must fully describe the weakness or deficiency and how it was discovered.

f. There shall be no external markings revealing the classification level of information being stored in a specific security container, vault, or secure room.

g. A Responsible Officer shall be appointed for each area where classified material is stored.

h. An access roster shall be posted on the exterior of the door for each open storage area. Personnel not listed on the roster must sign a visitor log and must be accompanied by an individual on the roster.

i. If necessary, the Responsible Officer or an individual authorized on the access roster shall be contacted to store any classified information received after hours. The CDO shall follow references (b) and (h) regarding receiving classified messages.

j. Storage containers will be inspected periodically.

k. Annual physical security surveys of areas containing classified information and/or material will be conducted by Physical Security.

l. "Locked/Open" signs (Optional Form 95) will be displayed on each container that contains classified material to indicate whether the container is locked or open.

m. Valuables such as money, jewels, precious metals, narcotics, etc., will not be stored in the same containers used to safeguard classified material.

n. Unclassified material will not be stored in the same containers used to safeguard classified material.

o. Unessential classified information will not be stored.

6. Combinations, Locks, and Keys

a. Guidance pertaining to combinations, locks, and keys is contained in chapter 10 of reference (b).

b. Combination changes, neutralization of lockouts and repairs, or maintenance of security containers will be requested through the Base Locksmith

by submission of a Work Request (Maintenance Management), NAVFAC Form 9-11014/20. Only trained personnel with the appropriate security clearance will make combination changes. Depending on the availability of trained security personnel the Command Security Manager can provide assistance for changing combinations upon request.

c. Records of combinations of containers with classified material will be sealed in a Security Container Information Envelope, SF 700 (figure 13-1), and kept on file in the G-3 EOC secure room. Combination envelopes to master containers and vault/safe rooms lending access to master containers will be turned in to the Security Manager for safekeeping.

d. When securing security containers, (vaults/strong rooms, safes, files, or cabinets) rotate dial or combination lock at least four complete turns in the same direction when securing.

e. When a container with a built in lock or a padlock is taken out of service, the built-in lock will be reset to the standard combination 50-25-50, and combination padlocks will be reset to the standard combination 10-20-30.

7. Procurement and Turn-in of Security Containers

a. New security containers will not be requested or requisitioned by activity heads if similar equipment is available from the Assistant Chief of Staff, G-4 or via the Security Manager.

b. When GSA approved security containers are no longer required or are not being used for storage of classified material, the using activity will turn in the container to the Assistant Chief of Staff, G-4 and notify the Command Security Manager.

c. The Command Security Manager will maintain listings of all security containers used for the storage of classified material. The Command Security Manager will be kept informed of all movements, change of possessions, and/or turn-ins of all approved security containers between and among divisions/activities/commands.

8. Destruction of Classified Information

a. Strict adherence to the procedures and methods for the destruction of classified material contained in Chapter 10 of reference (b) will be observed.

b. Destruction of classified information shall be accomplished by means that eliminate risk of recognition or reconstruction of the information.

c. The Command Security Manager will establish at least 1 day each year as "clean-out" day when specific attention and effort are focused on unessential classified and unclassified information.

e. Per reference (b), a record of destruction is not required for Secret and Confidential information.

9. Sensitive Unclassified Material, For Official Use Only, and Personally Identifiable Information

a. Information that is For Official Use Only (FOUO) and/or is sensitive but unclassified shall be controlled and safeguarded per reference (b).

b. Personally Identifiable Information (PII) shall be controlled and safeguarded per reference (i).

(1) Reporting procedures for loss or compromise of PII is contained in reference (i). Updated Personal Identifiable Information (PII) policy and breach reporting procedures are at https://hqdod.hqmc.usmc.mil/PII.asp. The Command Security Manager or the Privacy Act Coordinator will provide assistance with reporting loss or compromise of PII.

10. Loss or Compromise of Classified Information. The loss or compromise of classified information, including electronic spillage, presents a threat the national security. Immediately contact the Office of the Command Security Manager if this occurs. Chapter 12 of reference (b) contains reporting responsibilities and procedures for the loss or compromise of classified information.

Industrial Security Program

1. Basic Policy. Guidance concerning the Industrial Security Program is contained in references (a, b, and d).

2. Installation Access

a. Contractor employees will comply with installation access requirements in accordance with reference (d). Depot I.D. access badges will be issued for contractor and vendor employees who do not require a government computer account.

b. Common Access Cards will be issued in accordance with reference (e) for contractor employees requiring access to a government computer account.

3. Contractor Investigative Requirements for CAC Issuance and Fitness Determinations for Public Trust Positions

a. Investigations for contractor employees hired to perform unclassified duties will be processed per reference (a).

b. Contracting agencies and/or government contract representatives shall coordinate these procedures with the Office of the Command Security Manager.

4. Contract Requirements. Contracting agencies will ensure security requirements for installation access, government computer accounts, Common Access Cards, and/or access to classified information are written into all contracts.

5. Contracting Officer Representative (COR). The Contracting Officer will designate, in writing, one or more qualified security specialists as the Contracting Officer's Representative (COR). The COR is responsible to the contracting officer for coordinating with the security manager, 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 DD254 Contract Security Classification Specification document is prepared properly. The COR will ensure that all industrial security functions and requirements are accomplished when classified information is provided to industry for performance on a classified contract.

a. The DD254 will be signed by the COR. At no time will DD254s be accepted if found to be signed by the Facility Security Officer (FSO) or other contractor. The DD254 is invalid unless signed by a government official.

b. Copies of DD254 will be provided to all commands who are recipients of services provided by a classified contract. If not otherwise provided, Command Security Managers will contact the holder of the contract and obtain a copy of the original DD254 and all amendments for all classified contracts that authorize contractors to have access to classified information within

their commands to ensure validation of contractor security requirements and authorizations.

6. COR Training. The assigned COR will receive training within 30 days of assuming COR responsibilities. The Defense Acquisition University provides a web-based course entitled "COR with a Mission Focus," course number 'DAU CLC106.' The course may be found at the following website; https://acc.dau.mil/CommunityBrowser.aspx?id=31505. Other training opportunities may be available through sister services or other venues. Some research may be required.

7. Contractor access to classified information. The presence of contractors within a command with access to classified information must be supported by a valid DD254 and a valid Visit Request which identifies the contract and the individuals who will support the contract. Verification of clearance eligibility will be made via JPAS.

a. Access for contractors will be determined by the Commanding Officer. At no time will access entries in JPAS, made by the contracting company, be acceptable for the assignment of access to national security information.

b. Contractors with Temporary Access established by the Defense Industrial Security Clearance Office (DISCO) 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 information may be withheld.

8. Security training for contractors. Contractors who have access to classified information will 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. Conversely, if duties are performed at both the command and contractor facilities, the contractor may participate in the contractor's security training program. However, evidence of training participation must be furnished to the command to verify participation. Additionally, 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 will be grounds for suspension of access to classified information.

9. Continuous Evaluation for contractors. Contractors who are involved in issues which require reporting under reference (a), chapter 10, Continuous Evaluation, will be reported to DISCO by the command. Coordination should be made with the contractor's Facility Security Officer (FSO).