UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
POSTAL SERVICE CENTER BOX 8003
CHERRY POINT, NORTH CAROLINA 28533-0003

ASO 5510.2B
SEC
29 JUL 2022

AIR STATION ORDER 5510.2B

From: Commanding Officer, Marine Corps Air Station, Cherry Point
To: Distribution List

Subj: INFORMATION AND PERSONNEL SECURITY PROGRAM (IPSP)

Ref: (a) DoDM 5200.01, Volumes 1-3
(b) DoDI 5200.48 of 6 Mar 2020
(c) DoDM 5220.22 of 8 May 2020
(d) Homeland Security Presidential Directive 12 (HSPD-12)
(e) Committee on National Security Systems Instruction (CNSSI) No. 7003 of Sep 2015
(f) Information Assurance Publication 5239-22 of Sep 2008
(g) SECNAV M-5510.30C
(h) SECNAV M-5510.36B
(i) MCO 5510.18B
(j) MCO 5530.14A
(k) MCO 3302.1F
(l) Security Executive Agent Directive 3
(m) Security Executive Agent Directive 4

Encl: (1) Marine Corps Air Station Cherry Point Security Manual

1. Situation. To publish Marine Corps Air Station, Cherry Point (MCAS CHERPT) command policy addressing responsibilities and procedures for the management of information, personnel, physical, and industrial security. This Order is developed in accordance with the references.

2. Cancellation. ASO 5510.2A.

3. Mission

a. To publish uniform and effective security procedures in the application of information, personnel, physical, and industrial security disciplines. Each chapter will address a security discipline or a part of a discipline. Familiarity with the contents of all the references is essential in developing an understanding of the supplemental instructions contained herein.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. To set forth policies and establish procedures in support of MCAS CHER PT security program and provide all levels of management with guidelines for adherence to regulations.

(2) Concept of Operations. The Command Security Manager is on the Commanding Officer's Special Staff and will have access to serve as the principal advisor in matters pertaining to the Command's Security Program. The Command Security Manager will administer the Information and Personnel Security Program (IPSP) as contained herein and conduct annual internal reviews and inspections of each security discipline. Self-inspections will be conducted semi-annually as directed in reference (i). Independent inspections and inventories are typically conducted annually, as circumstances dictate, on all sections holding classified information and equipment.

b. Headquarters and Headquarters Squadron, MCAS CHERPT. Comply with the intent and content of this Order.

c. Coordinating Instructions. Recommended changes concerning this Order are invited and may be submitted to the Installation Commanding Officer via the appropriate chain of command.

5. Administration and Logistics. This Order incorporates all changes promulgated by the Secretary of Defense, Secretary of the Navy, and Commandant of the Marine Corps since publishing the previous Order.

a. This Order contains modifications designed to clarify and provide a more comprehensive understanding of the IPSP as it pertains to the mission of MCAS CHERPT.

b. This Order must be used in conjunction with references (a) through (h).

6. Command and Signal

a. Command. This Order applies to all Marines, Civilians, and contract support personnel within MCAS CHER PT command. Other requests for this document will be referred to MCAS CHERPT Command Security Manager.

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

M. R. HUBER

DISTRIBUTION: A

TABLE OF CONTENTS

CHAPTER 5 INFORMATION SECURITY POLICY AND PROCEDURES

CHAPTER 6 INDUSTRIAL SECURITY

CHAPTER 7 EMERGENCY ACTION PLANS FOR CLASSIFIED MATERIAL

CHAPTER 8 PHYSICAL SECURITY

Chapter 1

Responsibilities

1. Basic Guidance

a. MCAS CHER PT personnel will follow the guidelines and instructions set forth in the supporting documents from the Department of Defense (DoD), Department of the Navy (DON), and Headquarters Marine Corps (HQMC).

b. The Command Security Manager will adjust security policies and procedures as required when changes are made to orders and directives.

c. Vigilance by all military and civilian personnel of MCAS CHER PT is the principle security safeguard.

2. Definitions

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

b. Classified National Security Information. Information that has been determined pursuant to Executive Order 13526, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

c. Classified Material. Any matter, document, hard drive, magnetic tape, media, product, or substance on or in which classified information is recorded or embodied.

d. Continuous Evaluation. The process by which all military and civilian individuals who have established security clearance eligibility are monitored to ensure they continue to meet the loyalty, reliability, and trustworthiness standards expected of individuals who have access to classified information. This monitoring process relies on all personnel within a command to report unfavorable or potentially unfavorable information.

e. Custodian. A properly cleared individual with access to a specific category of classified material who has possession of, or is otherwise charged with, the responsibility of receiving, safeguarding, destroying, transferring, and accounting for classified information.

f. Information Security. The system of policies, procedures, and requirements in place to protect classified information that could reasonably be expected to cause damage to national security if subject to unauthorized disclosure. The term also applies to policies, procedures, and requirements established to protect Controlled Unclassified Information (CUI) that may be withheld from release to the public pursuant to Executive Order, statute, or regulation.

g. Defense Information System for Security (DISS). DISS tracks and contains all clearance related information for all DON personnel.

h. Need-to-Know. The determination that a prospective recipient requires access to specific

classified information in order to perform or assist in a lawful and authorized governmental function. It is the custodian's responsibility to determine the need-to-know before releasing classified information to any person.

i. Personnel Security Clearance. An administrative determination by the commander that an individual is eligible for access to classified information of a specific classification category. This is based upon the appropriate Personnel Security Investigation (PSI) and DoD Consolidated Adjudication Facility (DoDCAF) adjudication.

j. Classified Material Control Center (CMCC) Custodian. For the purpose of this Order, the CMCC Custodian is responsible for the control of classified material at this command. The CMCC Custodian must be consulted before receiving, reproducing, transmitting, or destroying collateral classified material in coordination with the governing orders and directives.

k. Security Incidents. There are two types of security incidents: violations and infractions. In either case, a security inquiry (SI) or investigation may be required to determine the circumstances of the incident and compliance with applicable directives and orders.

l. Spillage. Occurs whenever classified information or CUI is placed on an information 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 instruction.

3. Command Management. In compliance with references (a), (b), (g), (h), and (i), the Command Security Program has established a network of personnel with distinct responsibilities to supervise and ensure effective security, control, and utilization of classified material.

a. Control Officers. To ensure the proper handling and control of classified material, the following officers and their alternates, as appropriate, will be appointed in writing to manage the security program:

(1) Command Security Manager.

(2) Top Secret Control Officer.

(3) North Atlantic Treaty Organization (NATO) Control Officer.

(4) CMCC Custodians.

b. Program Managers, Supervisors, and Special Staff Officers

(1) Are responsible for security and continual review of security procedures and practices within their respective units and areas of responsibility.

(2) Will maintain adequate security for classified material, and ensure both military and

civilian personnel have an eligibility to access classified information and have a demonstrative need-to-know before handling classified material in the performance of their duties.

(3) Will ensure any adverse information concerning any member of their activity is brought to the attention of the Command Security Manager.

(4) Will recommend one security point of contact to coordinate security functions to the Command Security Manager. Alternate Security Coordinators may be recommended for appointment. The recommendation letter must have the signature of senior management within the program or staff office.

(5) Will ensure all of their military and civilian personnel with access to classified material attend and/or complete all training per the MCAS CHER PT Security Management annual training plan.

4. Safeguarding. Everyone is responsible for the security of classified information to which he or she has access. Each individual is responsible for reporting to the office of the Command Security Manager any violation of security regulations, security weakness, or security incidents of which they become aware. This can be accomplished in person, via email, or by phone call to any security member.

Chapter 2

Personnel Security Investigations, Access and Clearances

1. General. This Order provides the requirements for personnel security investigations, access authorization, and the administrative withdrawal, denial, or termination of security clearances or access for military and government civilian employees of this command.

2. Basic Policy. No person shall be granted access to classified material or assigned to sensitive duties unless a favorable determination has been made by the DoDCAF regarding loyalty, reliability, trustworthiness, and judgment. The initial determination will be based upon a PSI appropriate to the clearance level required for the position held and duties assigned.

3. Responsibilities

a. The Command Security Manager is responsible for the administrative preparation and submission of a PSI for MCAS CHER PT military and civilian personnel who have not been the subject of an earlier investigation.

b. Program Managers, Supervisors, and Special Staff Officers requesting security clearances or investigations of their personnel should contact the Command Security Manager for guidance in processing the requests. These requests must be aligned with the billet description for military personnel and position description for civilian personnel.

4. Policies and Procedures

a. No person appointed or retained as a civilian employee in the DoN or Marine Corps will be granted access to classified information or assigned to other sensitive duties that are subject to investigation under the provisions of security regulations unless such appointment, acceptance, retention, clearance, or assignment is clearly consistent with the interests of national security.

b. Appointment or retention in civilian employment and acceptance or retention in the Marine Corps shall be assumed to be clearly consistent with the interests of national security unless or until a determination has been made by competent authority that there is a reasonable basis for doubting the person's loyalty to the United States government.

c. Determinations of suitability or eligibility for civilian employment or service in the Marine Corps on any other basis are not personnel security determinations, and therefore, are not under the scope of this Order.

5. Investigations. Verification of a valid security investigation will be completed as part of the check-in process.

a. Military personnel are required to have a National Agency Check with Local Records Check (NACLC) or T3 performed by the Defense Counterintelligence and Security Agency (DCSA) and adjudicated by the DoDCAF for access to information and systems up to the Secret level.

b. Civilian personnel require an initial Access National Agency Check with Inquiries (ANACI), now known as a T3, or a follow-on NACLC, now known as a T3R reinvestigation, performed by DCSA and adjudicated by the DoDCAF for access to information and systems up to the Secret level.

c. Both military and civilian personnel required to have an initial Single Scope Background Investigation (SSBI), now known as a T5, or a follow-on Phased Periodic Reinvestigation (PPR), now known as a T5R, performed by DCSA and adjudicated by the DoDCAF for access to information and systems up to the Top Secret level.

d. To remain in compliance with the references, supporting contractors must have a favorably adjudicated NACLC/T3 (for Secret) or SSBI/T5 (for Top Secret) if classified access is required by their contract. Contractors requiring a Common Access Card (CAC) must have at least a National Agency Check with Inquiries (NACI/T1) opened. If the NACI/T1 returns unfavorably, the contractor CAC must be retrieved and revoked. Chapter 6 has more information on Industrial Security issues.

6. Investigation Process. PSIs take from three to 12 months on average to complete, depending on the type of investigation and the information provided by the individual. Investigations will not be performed on individuals whose expected date of separation from federal service is less than 12 months away.

a. Favorable. A favorable PSI indicates the individual is of good character, is loyal to the U.S. government, reliable, trustworthy, and of good judgment. An individual who has been the subject of a favorable PSI is eligible to hold the type of clearance appropriate to the level of investigation performed. The DoDCAF is solely responsible for the adjudication of all PSIs for MCAS CHER PT personnel.

b. Unfavorable/No Determination Made. An unfavorable PSI adjudication will result in the immediate loss of access to classified material. "No Determination Made" can result from several scenarios, but generally means a prior investigation was not completed or sufficiently satisfied. Either of these will require interaction between the employee, security personnel, and the DoDCAF.

7. Classified Access

a. Top Secret. Top Secret access may be granted to those individuals who have been the subject of a favorably adjudicated SSBI/T5, SBPR/T5R, or PPR/T5R investigation, and whose current position constitutes a need-to-know. Top Secret level investigations will be in compliance for six years after the closing date of the investigation. After the six-year period, individuals still requiring Top Secret access are required to submit a new investigation package. If Top Secret access is no longer required, Secret access eligibility remains for an additional four years.

b. Secret. Secret access may be granted to those individuals who have been the subject of a favorably adjudicated NACLC/T3 or T3R, ANACI/T3 or T3R, SSBI/T5, or PPR/T5R

investigation and whose position constitutes a need-to-know. Secret level investigations will be in compliance for ten years after the closing date of the investigation. After the ten-year period, individuals are required to submit a new investigation package.

8. Temporary Access. Individuals requiring temporary access must have their investigation submitted to DCSA, and have their Personnel Security Questionnaire screened with favorable fingerprints and approved by the Command Security Manager for an eligibility determination.

a. Individuals with adverse information; such as non-judicial punishment, offenses involving drugs or alcohol, or any other criminal conduct are not eligible for temporary access.

b. Individuals who have previously been the subject of an unfavorable PSI are not eligible to hold temporary access. Temporary access can be granted and removed by the Command Security Manager.

9. Administrative Withdrawal of Access. In agreement with the need to maintain the minimum number of cleared personnel consistent with mission requirements, Program Managers, Supervisors, or Special Staff Officers must notify the Command Security Manager of any person who no longer requires access to classified information due to a job change within the command, a change in duties, or for any other justifiable reason. When classified access is administratively withdrawn, the appropriate entry will be made in both the individual's personnel security file and in DISS. Administrative withdrawal of an individual's access has no negative bearing on future clearance eligibility.

10. Clearance Denial or Revocation for Cause

a. When it is determined an individual does not meet or no longer satisfies the requirements for a security clearance, the security clearance will be denied or revoked by the DoDCAF.

b. All due process provisions will be afforded to the individual.

c. The Command Security Manager will be the primary point of contact (POC) for the individual and the DoDCAF through the denial or revocation process.

d. The Commanding Officer may withdraw access to classified information when an employee has committed a security violation, a disciplinary infraction, or caused a security incident.

11. Access

a. The Commanding Officer will grant access to classified information to an individual who has an official need-to-know, valid clearance eligibility, and for whom there is no disqualifying information.

b. Prior to granting access to classified material, the individual's supervisor must request access through the Command Security Manager.

c. The request should clearly articulate the classified access requirement and must be signed by the individual's supervisor. Once signed, send the request to the Security Management Office (SMO) for continued processing. SMO is not the access-granting authority, but facilitates the enabling or disabling of access as requested or required by appropriate leadership personnel.

12. Visit Requests. All incoming visitors that require access to classified information or areas must submit a Visit Request via DISS to SMO Code 001466 for non-SCI. MCAS CHER PT does not operate at the SCI level; therefore, no SCI visits will be submitted.

13. Foreign Travel Notification. All personnel, civilian and military, will notify the Antiterrorism Officer (ATO) and Command Security Manager of their intent to either go on official government business or personal travel outside of the Continental U.S. (OCONUS) no less than 30 days prior to their departure date.

14. Reporting Requirements

a. All command personnel are required to report unfavorable information to both their supervisor and the Command Security Manager as soon as the information becomes available. Reportable personnel security issues are explained below in section (b).

(1) In addition to self-reporting, personnel have an obligation to report derogatory information about another employee once they are aware of the information. This includes information on co-workers, supervisors, subordinates, contractors, or visitors.

(2) The Command Security Manager is required to report all derogatory/unfavorable information to the DoDCAF without attempting to mitigate the information first.

(3) The DoDCAF will then decide whether to favorably re-adjudicate the individual's eligibility or to begin the adverse determination process.

(4) SMO's jurisdiction over the matter ends once reported, but SMO will remain the primary point of contact between the individual and the DoDCAF as long as the person is assigned to MCAS CHER PT.

(5) If an individual resigns or retires prior to the DoDCAF making an adjudicative decision, the DoDCAF will enter a "Loss of Jurisdiction" entry into DISS, which will end any adjudicative decision making process.

b. The following security issues must be reported to Security immediately:

(1) Involvement in activities which or sympathetic associations with persons who unlawfully practice or advocate the overthrow or revision of the U.S. government 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, unreliability, untrustworthiness, or unwillingness to comply with rules and regulations, or unwillingness to cooperate with security clearance processing.

(6) Unexplained affluence or excessive indebtedness.

(7) Alcohol abuse or alcohol-related incidents.

(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 activities that could cause a conflict of interest.

(13) Misuse of Information Technology (IT) Systems.

c. Further information on items above can be found in references (l) and (m), Security Executive Agent Directives 3 and 4.

15. Continuous Evaluation Program

a. All activities will report questionable or unfavorable information to the Command Security Manager for reporting to DoDCAF.

b. If the developed information is significant enough to require a suspension of the individual's access for cause, the suspension action will be accomplished in accordance with reference (g) using the proper administrative chain-of-command.

c. A command report of local access suspension for cause will automatically result in suspension of the individual's clearance eligibility by the DoDCAF. Once clearance eligibility is suspended or the individual is debriefed from access for cause, the individual may not be granted access or considered for re-indoctrination until clearance eligibility has been reestablished by the DoDCAF.

d. The Command Security Manager will act as the go-between in matters involving the DoDCAF.

Chapter 3

Administrative Measures

1. Requirement. As directed by references (a), (g), (h), and (i), all MCAS CHER PT personnel, civilian and military, are individually responsible for complying with the provisions of this Order and reporting any security incidents involving classified information.

2. Incidents Subject To Penalties

a. Military and civilian personnel of the DON are subject to administrative penalties if they:

(1) Knowingly, willfully, or negligently disclose classified information or CUI to any unauthorized person, organization, system, country, or state.

(2) Knowingly, willfully, or negligently violate any provision of the governing orders and directives established by the DoD, DoN, HQMC, or this Order.

b. Penalties include, but are not limited to: a warning notice, a reprimand, suspension without pay, forfeiture of pay, and removal or discharge. Penalties will be imposed upon any person who is responsible for one of the above-specified violations, regardless of grade or level of employment, and as appropriate to the particular case, In accordance with applicable law and regulations.

c. Security violations and incidents reflect negatively on an individual's clearance eligibility and may affect continued access to classified information. Security incidents can be cause for denial or revocation of the individual's clearance eligibility even when the violations are not separately punishable.

d. The unauthorized disclosure or spillage of CUI will be handled in accordance with reference (b), which also includes any amplifying protection and handling guidance for specific types of CUI required by law or federal regulation.

3. Corrective Action. The DoN has indicated appropriate corrective action will be taken whenever:

a. A violation occurs, or when repeated administrative discrepancies, neglect, or disregard of requirements occurs.

b. The Command Security Manager will ensure a security investigation is conducted within the requirements outlined in DoD, DoN, and HQMC regulations and with directives of the governing orders and directives for all security violations.

4. Administrative Discrepancies

a. Repeated administrative discrepancies in the handling of classified material that are determined not to constitute an incident under section 5 may be grounds for adverse administrative action including warning, admonition, or reprimand, as appropriate.

b. Administrative discrepancies include failure to use appropriate cover sheets; using incorrect classification markings and dates for declassification; failure to properly mark working papers; failure to submit timely inventories; failure to initial the Security Container Check Sheet, Standard Form (SF)-702; or other repeated neglect or disregard of requirements of this Order.

5. Security Incidents and Violations

a. There are three types of security incidents:

(1) Willful Violations. Security incidents that indicate a person purposefully disregarded DoD, DoN, and/or HQMC security information safeguarding policies, or requirements that resulted in, or could be expected to result in, the loss or compromise of classified information.

(2) Negligent Violations. Security incidents that indicate a person acted unreasonably in causing the spillage or unauthorized disclosure; such as a careless lack of attention to detail, or reckless disregard for proper procedures.

(3) Inadvertent Violations. Incidents where the person did not know that the security violation or unauthorized disclosure was occurring; such as when someone reasonably relied on improper markings.

b. Some security requirement infractions involve a failure to comply that cannot reasonably be expected to and does not result in the loss, compromise, or suspected compromise of classified information. An infraction may be unintentional or inadvertent.

(1) While it does not constitute a security violation, if left uncorrected, infractions can lead to security violations or compromises.

(2) An infraction requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

c. A security violation obviously presents the greater threat to national security as the unauthorized disclosure of classified information or CUI poses a significant threat to national security and to DoD, DoN, HQMC and MCAS CHER PT operations and missions.

(1) Security incidents of either type will be reported, and the issues causing the incident will be corrected rather than covered up.

(2) If responsibility is demonstrable, the offender(s) will be appropriately disciplined.

6. Disciplinary Action

a. The disciplinary action if a security violation by military personnel will be determined by the appropriate authority.

b. There is no schedule of disciplinary actions for civilians, but rather a range of actions extending from informal admonishment to removal. This extensive range permits actions of varying degrees of severity.

c. Any person who violates a security regulation is subject to disciplinary action. The punishments for breaches of security for civilian personnel are listed below.

(1) Failure to safeguard classified material resulting in a security compromise:

(a) First Offense. Reprimand.

(b) Second Offense. Temporary Access Suspension (TAS).

(c) Third Offense. Local access suspension.

(2) Failure to safeguard classified material not resulting in a security compromise:

(a) First Offense. Verbal Reprimand.

(b) Second Offense. Reprimand to TAS.

(c) Third Offense. Local access suspension

d. In addition to the possible disciplinary actions outlined above, 18 U.S.C., §798 informs all personnel that unauthorized disclosure of classified information may result in a fine of not more than $10,000 or imprisonment for not more than ten years, or both, per occurrence.

Chapter 4

Security Education and Training

1. Requirements. Implement, as directed by references (a), (g), (h), and (i), an active security education program to instruct all personnel in security policies and procedures. All civilian employees and military personnel are required to attend/complete the annual security training when scheduled. Failure of individuals to complete the training requirements mentioned above could result in the loss of access until compliance is achieved. WAIVERS WILL NOT BE GRANTED.

2. Command Security Manager Responsibilities

a. Formulates and coordinates the security education program and is responsible for ensuring personnel receive the required security training.

b. Monitors the program, obtains training aids and program materials, and assists in presentations.

3. Security Briefings and Training

a. At a minimum, the following required security briefs and training will be conducted for command personnel.

(1) Local Orientation Briefing. A local orientation security briefing will be conducted for all newly joined personnel by the Command Security Manager or one of his/her representatives. This briefing will be a part of the check-in process and will provide new personnel an awareness of basic requirements for the protection of classified information and Command security procedures.

(2) Annual Refresher Briefing. A general security refresher-training brief will be conducted annually for all Command personnel by the Command Security Manager or his/her staff.

(3) NATO Security Clearance Briefing

(a) All civilian employees and military members who have classified access will be required to receive a NATO awareness security brief. This briefing provides guidance concerning how to protect NATO classified material if the individual happens to be exposed to it inadvertently.

(b) All civilian employees and military members who are required to review and handle NATO material will be required to have read and acknowledged the NATO security brief.

(4) Special Access Briefings. Any civilian employee and military member whose duties require access to special types of information; such as NATO, or other special access programs,

must be briefed prior to access to the information. The Command Security Manager or his/her representative will conduct or coordinate the Special Access Briefings.

(5) Debriefings. Personnel who have had access to classified and CUI shall be debriefed prior to transfer, termination of active military service or civilian employment, or temporary separation for a period of 60 days or more, including leave without pay.

(6) One-Time Special Security Briefings. From time to time, as new information concerning security regulations and procedures is received from higher authority, the Command Security Manager will schedule special training sessions for the organizational groups affected by the new security information.

(7) Foreign Travel Briefings. Foreign travel briefings are normally provided by the resident ATO personnel located at MCAS CHER PT prior to traveling overseas. ATO personnel will determine if a foreign travel brief/debrief is necessary dependent upon the country being visited.

b. Security Professionals. The Security Professional Education and Development (SPED) Certification Program is part of the DoD initiative to professionalize the security workforce. This initiative is to ensure there is a common set of competencies among security experts that promotes cooperation, facilitates professional development and training, and develops a workforce of certified security professionals.

c. On-The-Job Security Training. For all other personnel, online training and other resources are available through the CDSE, which may be accessed at https://cdse.usalearning.gov/. A number of these training courses have acquisition points. Courses may be virtual or in person, instructor led or self-paced.

Chapter 4

Security Education and Training

1. Requirements. Implement, as directed by references (a), (g), (h), and (i), an active security education program to instruct all personnel in security policies and procedures. All civilian employees and military personnel are required to attend/complete the annual security training when scheduled. Failure of individuals to complete the training requirements mentioned above could result in the loss of access until compliance is achieved. WAIVERS WILL NOT BE GRANTED.

2. Command Security Manager Responsibilities

a. Formulates and coordinates the security education program and is responsible for ensuring personnel receive the required security training.

b. Monitors the program, obtains training aids and program materials, and assists in presentations.

3. Security Briefings and Training

a. At a minimum, the following required security briefs and training will be conducted for command personnel.

(1) Local Orientation Briefing. A local orientation security briefing will be conducted for all newly joined personnel by the Command Security Manager or one of his/her representatives. This briefing will be a part of the check-in process and will provide new personnel an awareness of basic requirements for the protection of classified information and Command security procedures.

(2) Annual Refresher Briefing. A general security refresher-training brief will be conducted annually for all Command personnel by the Command Security Manager or his/her staff.

(3) NATO Security Clearance Briefing

(a) All civilian employees and military members who have classified access will be required to receive a NATO awareness security brief. This briefing provides guidance concerning how to protect NATO classified material if the individual happens to be exposed to it inadvertently.

(b) All civilian employees and military members who are required to review and handle NATO material will be required to have read and acknowledged the NATO security brief.

(4) Special Access Briefings. Any civilian employee and military member whose duties require access to special types of information; such as NATO, or other special access programs,

must be briefed prior to access to the information. The Command Security Manager or his/her representative will conduct or coordinate the Special Access Briefings.

(5) Debriefings. Personnel who have had access to classified and CUI shall be debriefed prior to transfer, termination of active military service or civilian employment, or temporary separation for a period of 60 days or more, including leave without pay.

(6) One-Time Special Security Briefings. From time to time, as new information concerning security regulations and procedures is received from higher authority, the Command Security Manager will schedule special training sessions for the organizational groups affected by the new security information.

(7) Foreign Travel Briefings. Foreign travel briefings are normally provided by the resident ATO personnel located at MCAS CHER PT prior to traveling overseas. ATO personnel will determine if a foreign travel brief/debrief is necessary dependent upon the country being visited.

b. Security Professionals. The Security Professional Education and Development (SPED) Certification Program is part of the DoD initiative to professionalize the security workforce. This initiative is to ensure there is a common set of competencies among security experts that promotes cooperation, facilitates professional development and training, and develops a workforce of certified security professionals.

c. On-The-Job Security Training. For all other personnel, online training and other resources are available through the CDSE, which may be accessed at https://cdse.usalearning.gov/. A number of these training courses have acquisition points. Courses may be virtual or in person, instructor led or self-paced.

Chapter 5

Information Security Policy and Procedures

1. Policy. The Information Security Program is established, as required by references (a), (b), (h), and (i), to ensure information classified under the authority of Executive Order (E.O.) 13526 is protected from unauthorized disclosure. This program applies uniform and consistent policies and procedures to the classification, safeguarding, transmission, and destruction of classified information.

2. Authority

a. The Commanding Officer (CO), MCAS CHER PT is responsible for establishing and maintaining an Information Security Program in compliance with the references.

b. The responsibility for the security and proper handling of classified material extends directly to military and civilian personnel having knowledge or possession of such material and to program managers and supervisors within whose scope of classified material is utilized.

c. Individual requests for guidance or interpretation of this Order should be addressed to the CO, MCAS CHER PT, Attn: Command Security Manager.

3. Applicability

a. This chapter establishes coordinated policies for the security of classified information, by incorporating the policies of numerous DoD, DON, and HQMC directives. It is not expected that these directives will or can ensure absolute security at MCAS CHER PT. Rather, they permit the accomplishment of essential tasks while affording selected items of information reasonable degrees of security with a minimum risk.

b. As this chapter establishes coordinated policies for maintenance of the program, it is applicable to all organizations and activities under the purview of the Commander. References (a), (b), (h), (i), and this Order will provide the basis for managing the MCAS CHER PT Information Security Policy and Procedures.

4. Responsibility for Compliance

a. The Command Security Manager is responsible for compliance with and implementation of this Order.

b. Program Managers and Supervisors are responsible for compliance with and implementation of this Order within their areas of responsibility.

c. Each individual, military, civilian, or contractor, employed through the Navy or Marine Corps, is responsible for compliance with this Order in all respects.

d. All activities that hold classified information are required to be registered as a Secondary Control Point (SCP) with the CMCC and have on-hand hard copies of the appropriate references and this Order.

(1) Upon determination of transferring, retiring, resigning or being reassigned, SCPs will immediately notify the CMCC in order to coordinate a timely and efficient inventory and turnover of sub-custody material.

(2) Newly assigned SCPs must be approved, assigned, and briefed by the CMCC prior to receiving any sub-custody material.

e. SCPs are responsible for the actions of all personnel assigned to them and those who may be in use of the classified material in their care.

5. Storage

a. Classified information will be stored only in a General Service Administration (GSA) approved security container, in approved areas, on accredited IT systems, and under conditions that 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 information is processed or stored.

(1) Secure Rooms (SR) will be designated in writing by the MCAS Command Security Manager following the completion of a Physical Security Survey (PSS) conducted in accordance with reference (i). All designated SRs must also be designated as a Restricted Area in accordance with reference (i).

(a) All personnel will comply with need-to-know policy for access to classified information.

(b) Weapons or pilferable items such as money, jewels, precious metal, or narcotics will not be stored in the same security container used for the storage of classified material.

(c) Classified material will also not be stored with UNCLASSIFIED, UNCLASSIFIED//FOR OFFICIAL USE ONLY, CUI or any other material.

6. Classification Management

a. MCAS CHER PT does not have Original Classification Authority (OCA). All classification actions within MCAS CHER PT are derivative in nature. In accordance with reference (i), any person with appropriately assigned clearance eligibility and approved access to classified information may act as a derivative classifier. In order to support this authority, the following requirements must be met.

(1) Training. Refer to chapter 4 of this Order for training requirements.

(2) Marking. Mark all classified material derived within MCAS CHER PT in accordance with Volume 2 of reference (a).

7. Classified Material Controls

a. All Top Secret CMI (including copies) received by MCAS CHER PT and subordinate commands shall be continuously accounted for, individually serialized with a locally developed control number and entered into a command Top Secret Control Log. The log shall completely identify the information, and at a minimum, include the date originated or received, individual serial numbers, copy number, title, change number if applicable, originator, number of pages, disposition (i.e., received, transferred, destroyed) and date of each disposition action taken. The Top Secret Control Log will be retained for five years after the material is transferred, or destroyed.

(1) Retention of Top Secret documents within MCAS CHER PT and subordinate commands will be kept to a minimum. When Top Secret CMI is destroyed, the CMCC section will prepare a Classified Material Destruction Report, OPNAV 5511/12 identifying the material destroyed and the two officials who witnessed its destruction, and their signatures. The TSCO will retain these destruction records for a period of five years.

b. Secret and Confidential Controls

(1) The Command Security Manager is the CMCC Custodian and is responsible for controlling classified material entering, leaving, or being created at MCAS CHER PT.

(2) Any expected inbound classified material will be reported to the Command Security Manager as soon as the project POC is aware of it.

(a) Receive. The Command Security Manager and Alternate Custodian are the only authorized recipients of classified United States Postal Service (USPS) Registered Mail, Express Mail, and Courier Packages.

(b) Only the CMCC Custodian or Alternate will open these mail pieces. If a package is received and is incorrectly issued to an unauthorized recipient, that recipient will proceed directly to the CMCC with the package and all wrappings.

(c) The CMCC Custodian will then verify the contents of the package matches the transmittal receipt and return the receipt to the sender.

1. Control Numbers. The CMCC Custodian will mark the classified material with a control number, attach SF-707 Secret Classification Sticker, if required, and will annotate all required information from the item(s) into the CMCC Database.

2. Dissemination. The Command Security Manager will issue the classified material to the appropriate sub-custodian to include colored cover sheets as required. Any dissemination of classified information outside the command must be approved by the Command Security Manager.

(3) The SCPs are responsible for the classified material and will handle, store, and use the material in accordance with all current policies and regulations. Any changes in the location, SCPs, project, or status of the classified material will be reported to the CMCC immediately.

(4) When a file, folder, or group of classified documents is removed from secure storage, it must be conspicuously marked with the highest classification of any classified document it contains and have an appropriate classified document cover sheet attached.

(5) The only document cover sheets authorized for use by activities at MCAS CHER PT are as follows:

(a) Top Secret, SF 703 - NSN 7540-01-213-7901

(b) Secret, SF 704 - NSN 7540-01-213-7902

(c) Confidential, SF 705 - NSN 7540-01-213-7903

(6) Inventory. The CMCC Custodian manages the entire classified material inventory and requires all SCPs to conduct internal inventories annually.

(7) Safeguarding

(a) The Command Security Manager will conduct an annual inventory of GSA security containers to ensure their structural integrity and proper use.

(b) The Command Security Manager will ensure all SCPs are trained on proper safeguarding requirements and that all updated policies and procedures are located in a public location for all users to review.

(8) Classified material (hard drives) no longer needed for any reason will be destroyed with the CMCC Custodian present at Bldg 151 using approved industrial shredder. All other classified material, to include cd's and documents, will be turned over to the CMCC Custodian for destruction in bldg. 1, rm 1079. Once the CMCC Custodian takes responsibility for the classified material, the SCP is no longer responsible.

(9) All classified material generated, to include working papers, at this Command must be properly portion marked with all classification markings required and controlled immediately after creation.

(10) Classified material will only be signed out to individuals during day-to-day operations that utilize the material and who can account for its safe handling, storage, and protection when not in use.

8. Transfer or Transmission of Secret and Confidential Material

a. All classified material mailed via USPS Registered Mail will be received by the CMCC Custodian. The CMCC Custodian will coordinate with Supply and/or Mail Room for delivery of classified material packages to ensure complete control of the material.

b. If Supply or the Mail Room notifies a person that a package has arrived and that user suspects the package contains classified materials, that Supply Clerk, Mail Clerk, or person must immediately notify the CMCC Custodian.

(1) If the Mail Clerk delivers a package to a person and upon opening the package, it contains classified information, that individual will immediately deliver the package with all wrappings and registered mail receipt to the CMCC Custodian.

(2) Do not tamper with the interior wrapper that identifies the package as classified material.

c. When informing anyone outside the Command to mail classified material by USPS to MCAS CHER PT, the address provided below is to be used.

(1) The correct mailing address for USPS containing classified information should read as follows:

(a) Outer Envelope:

Commanding Officer, MCAS Cherry Point
Attn: Command Security Manager
PSC Box 8003
Cherry Point, NC 28533-0003

(b) Inner Envelope:

Point of Contact/Project (on interior label only)
PSC Box 8003
Cherry Point, NC 28533-0003

(2) Never have the classified information mailed directly to an individual.

d. Transmission of NATO Classified Material

(1) Requests to send NATO classified material to personnel or activities outside the Command will be processed via the NATO Control Point Officer in the CMCC.

(2) NATO information must be stored separately. It cannot be commingled with U.S. classified information.

(3) Authority to hand-carry any NATO classified material OCONUS, its territories or Canada, on commercial aircraft must be approved by HQMC. NATO classified material must be packaged separately from other classified material and the inner envelope marked "NATO" along with the classification marking. Only the activity address of the courier will be shown on the outer envelope or wrapping.

(4) A continuous chain of receipts is required to record the movement of all NATO Secret material. The Communication Security (COMSEC) Custodian will maintain receipts on COMSEC material. The CMCC Custodian will maintain receipts on NATO.

e. The Command Security Manager will provide written authorization to individuals required to escort or hand-carry classified information. This authorization may be the DD Form 2501, Courier Authorization Card, included on official travel orders, or a courier authorization letter and is prepared by the SMO. Any of these three written authorizations may be used to identify appropriately cleared DoD military and civilian personnel approved to escort or hand-carry classified information; Special Access Program (SAP) and SCI information are excluded, between DoD commands subject to the following conditions:

(1) The individual has a recurrent need to escort or hand-carry classified information.

(2) The expiration date may not exceed three years from the issue date; pertains only to DD 2501.

(3) The individual must return the hand-carry authorization to the SMO upon transfer, termination of employment, or when authorization is no longer required.

f. The written authorization is intended for use between DoD commands worldwide and provides sufficient authorization to hand-carry classified information aboard a U.S. military aircraft.

g. Every precaution must be taken to prevent unauthorized disclosure when individuals are hand-carrying classified material in an official travel status.

h. If the movement requires transportation, the CMCC Custodian shall double wrap the classified material. A locked carrying-case or bag may be considered as the outer double wrapping, except when hand carrying aboard commercial aircraft.

i. MCAS CHER PT personnel requiring a Courier Card must meet with the SMO at least two weeks prior to date of departure. They will complete the Courier Advisory Acknowledgement before being issued a Courier Letter or Courier Card and to ensure the classified package will be ready for pickup on date of departure.

(1) It is mandatory for the Courier to check in with the CMCC prior to departure and immediately after returning from couriering classified information.

(2) The Courier Card or Courier Letter must be returned to the SMO upon expiration, upon departure from the Command, or upon completion of the mission in which the Courier Card or Courier Letter was required.

j. Any classified material brought into this Command after hours, or when the CMCC Custodian or Alternate are unavailable, will be checked in with the Command Duty Officer (CDO) and stored appropriately in a secured room or security container until the material can be processed through the CMCC. The CDO will contact the CMCC Custodian of the material so it can be retrieved for proper storage and assignment, as required.

k. Classified information will not be discussed via telephone except as authorized on approved secure communication devices; such as Secret-Voice over Internet Protocol (S-VoIP), telephone equipment and will not be transmitted via unapproved unclassified facsimile equipment.

9. Inspections and Inventories

a. The Command Security Manager will conduct announced and unannounced inspections of Level I and II Restricted Areas.

b. To ensure there is no introduction of prohibited items or contraband into secure working areas and the CMCC, and to deter the unauthorized removal of classified material, the following is provided:

(1) Prohibited items include personal or government equipment including:

(a) Laptops, computers, Personal Digital Assistant (PDA), and media;

(b) Photographic, video, and audio recording equipment;

(c) Two-way radios, pagers, cellular telephones, and personal wearable fitness devices.

c. Contraband items are commonly defined as goods prohibited by law from being imported or exported. There are many different kinds of contraband, including homemade weapons, gambling paraphernalia, excessively metered envelopes, weapons, drugs, and food.

d. Containers holding classified material are subject to random and unannounced inspections. The CMCC Custodian may require inventories and conduct an inventory at any time.

e. The CMCC Custodian will maintain records of Top Secret inventories for five years and two years for Secret inventories.

10. Reproduction

a. All classified information will be printed on colored paper. All Secret information will be printed on yellow paper.

b. Reproduction of classified information must be accounted for with the SCPs and CMCC within MCAS CHER PT.

c. Classified information will only be reproduced to the extent required for operational necessity unless restricted by the originating agency or for compliance with applicable statutes or directives.

11. Classified Meetings and Briefings

a. Classified meetings or briefings will be coordinated by the MCAS CHER PT host with the MCAS CHER PT SMO.

b. Personnel inviting guests from other organizations are required to notify Security via the visitor processes, whichever applies, to ensure proper vetting can be completed prior to guest arrival.

c. Foreign Visitors. A foreign visit is any contact by a foreign national or foreign representative that involves substantive or technical discussions or information. Avoid entering into these types of discussions with foreign persons or their representatives on initiatives that will result in the disclosure of classified information or CUI without first obtaining approval.

(2) For all requests for foreign official visits, requests will be submitted through the sponsoring government's Embassy.

d. All classified notes will be turned in to the meeting host at the end of the meeting along with the person's name, phone number, and organization's mailing address. The meeting host at the end of the meeting will enclose all the classified notes within a carrying case and deliver to the CMCC Custodian prior to that person's departure and for mailing to his/her security office, if necessary.

e. Personal Electronic Device (PED)

(1) It is the responsibility of MCAS CHER PT personnel hosting/sponsoring a classified meeting to inform their visitors of the MCAS CHER PT PED Policy.

(2) PEDs in restricted areas are not authorized and it is recommended that personnel leave their PEDs in their locked vehicles or, if available, locked within lockboxes located near the meeting room.

12. Printing from MCEN-S Computers

a. Personnel utilizing their MCEN-S accounts within MCAS CHER PT facilities have printing permissions and are required to coordinate with their SCP or CMCC to document holdings.

(1) The MCEN-S user must understand that they will apply all requirements listed in the Marking Classified National Security Information booklet and reference (a), Volume 2 prior to requesting to print.

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

(1) IT systems include 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 of data or information.

(2) Electronic media includes universal serial bus drives, flash drives, pen drives, compact disks, etc. which are not authorized on MCEN-S equipment.

(3) IT systems that process classified data, in forms other than traditional documents, such as weapons, navigation, and communication systems also require appropriate marking.

(4) All classified working papers will be controlled, logged in the Working Papers Logbook, maintained by the CMCC Custodian and only up to 180 days, and then turned into the CMCC for destruction or processed as a classified document. It is strongly encouraged that working papers are maintained for the minimum amount of time necessary.

13. Discovery of Suspected Classified Data Found Adrift. Any materials discovered by MCAS CHER PT personnel that are unlabeled, unknown, or potentially classified will be turned into the CMCC Custodian for immediate investigation/destruction.

14. Destruction Requirements

a. All material will be destroyed when it is no longer needed.

b. The National Security Agency (NSA) product list of approved crosscut shredders for destruction of classified information can be requested through the Command Security Manager. The Command Security Manager will approve the request prior to classified shredding within MCAS CHER PT.

c. Command Security Managers will use an NSA approved crosscut shredder that will reduce the information to shreds no greater than five square millimeters.

d. Strip shredders are not authorized for the destruction of classified information.

e. Destruction of unclassified sensitive data and CUI documents will be destroyed by utilizing a crosscut shredder or any means that would make it difficult to recognize or reconstruct the information.

f. Electronic media will be destroyed with the CMCC Custodian at bldg. 151 where they have equipment to degauss and shred hard drives and other types of electronic equipment.

15. Clean-out Day. The Command Security Manager will establish at least one day each year as a clean-out day, when specific attention and efforts are focused on disposition of unneeded classified information and CUI. Typically this day will be after the fiscal year near the holiday season. A memorandum for the record will record the clean-out date.

16. Working Papers. Secret and Confidential working papers are documents and material accumulated or created in the preparation of a deliverable; such as meeting notes, draft documents, and draft PowerPoint presentations. Working papers are marked in the same manner as a finished document at all times. All working papers will be reviewed by the Command Security Manager for proper markings before being released by the originator outside the originating command.

a. Working papers that contain Top Secret, SCI, or SAP information must be generated and maintained inside a Secure Compartmentalized Information Facility (SCIF). This level of working papers will not be generated within this Command.

b. All Secret and Confidential material held by the Command will be logged into the CMCC and accounted for. The one exception is the classified information maintained on the SIPR server.

c. Working papers will be maintained for less than 180 days or filed permanently.

17. Pre-Publication Review. All material prepared for public release in any format will be subject to an internal Command Security Review per the current edition of the DON Freedom of Information Act Program. Release will be provided unless one of the nine exemptions and/or three exclusions apply.

18. Controlled Unclassified Information (CUI)

a. CUI is information requiring safeguarding or dissemination controls pursuant to and consistent with law, regulations, or government policies in accordance with reference (b), but does not meet the requirements for classified information as required by Volume 1 of reference (a).

(1) This section provides supplemental policy for the handling and protection of CUI within MCAS CHER PT as required by reference (b).

(2) All military, civilian, cleared and uncleared contractors are individually responsible for compliance with the requirements outlined in this chapter.

(3) CUI must be identified and protected from unauthorized disclosure, appropriately designating, marking, safeguarding, disseminating, decontrolling, and destroying information.

b. Controls of CUI. Refer to reference (b) for policy on identification, access, safeguarding, marking, decontrolling, and dissemination of CUI.

c. Education and Training. All MCAS CHER PT personnel, military, and civilians; to include cleared and uncleared contractors, will receive CUI education and training which provides knowledge of CUI. The training will be inclusive with the command's orientation, indoctrination, and annual refresher training.

d. Destruction of CUI. As required by reference (b), CUI must be destroyed by any of the means approved for the destruction of classified information or by any other means which would make it difficult to recognize or reconstruct the information. Contact the Command Security Manager for assistance prior to purchasing any shredders for the destruction of CUI.

Chapter 6

Industrial Security

1. General. The National Industrial Security Program (NISP) was established to safeguard classified information that is released to industry to ensure the protection is maintained as required by E.O. 12829.

2. Responsibilities. As required by references (a), (b), (c), (g), (h), and (i), Program Managers and supervisors which are identified as government activities in this chapter will establish procedures as outlined that include appropriate guidance, consistent with reference (c) and this Order, to ensure that classified information released to industry is safeguarded.

a. The government activity, via the Command Security Manager, may deny access, for contract employees, to areas and information under their control for cause.

(1) Suspension or revocation of contractor security clearances can only be effected through the DoDCAF Industry Division.

(2) Any actions taken to deny a contractor access to areas and information will be reported to the Contracting Officer Representative (COR).

b. Contractors are required to have either a final or interim security clearance, in order to have access to classified information at MCAS CHER PT. In addition, contractors granted access to classified COMSEC or NATO material must hold a final security clearance for the level of classification involved.

c. Responsibility for initiating and submitting the request for a security investigation to the Defense Counter Intelligence Agency (DCSA) in support of classified access lies with the company's Facility Security Officer (FSO). This includes requests for initial security investigations and periodic reinvestigations.

3. Access. DoD Contractors will perform work within MCAS CHER PT in one of the following ways:

a. When a contractor is designated as a short or long-term visitor, the DoD Contractor must comply with MCAS CHER PT security regulations and shall be included in the MCAS CHER PT security education program.

b. When the contractor has a tenant seat within MCAS CHER PT spaces; such as when the contractor has sole occupancy of a space that is controlled and occupied by the contractor, the government activity shall assume responsibility for security oversight over classified work carried out by the cleared DoD contractor employees in their area. Additionally, the government activity is responsible for all security aspects of the contractor's operations in the work area and within the Command's area of responsibility.

4. Check-In. Prior to any DoD contractor reporting aboard for a dedicated seat assignment, the Contracting Officer will coordinate with the MCAS CHER PT SMO with the appropriate documentation required.

5. Escorting Privileges. Only DoD civilian and military personnel, whose principal place of work is within MCAS CHER PT, are authorized to escort visitors and contractor personnel within MCAS CHER PT areas.

a. Individuals must be thoroughly briefed in their responsibilities as an escort prior to performing the duty. The SMO conducts this training.

b. Escorts will announce that a visitor is in the area so that co-workers can turn over, cover, or store CUI material.

c. Escorts will walk with the individual under escort; and visually observe the individual under escort until the visitor leaves MCAS CHER PT or another escort assumes the duty.

d. Waivers to escort policy and procedures may be granted by the Command Security Manager or designee on a case-by-case basis.

6. Contract Security Classification Specification (DD Form 254) The government activity shall ensure that a DD Form 254 is incorporated into each contract that is handling classified information or material. The DD Form 254 is a legal document and part of the contract.

a. The DD Form 254, with attachments, supplements, and incorporated references, is designed to provide a contractor with the security requirements and classification guidance needed for performance of a classified contract.

b. An original DD Form 254 will be issued with each request for proposal, other solicitations, contract award, or follow-on contract to ensure that the prospective contractor is aware of the security requirements and can plan accordingly.

c. A Follow-On contract is a contract that is awarded to the same contractor for the same item or services as a preceding contract. A revised DD Form 254 will indicate the new contract number and authorizes the contractor to transfer material received or generated under the preceding contract to the new contract.

d. A revised DD Form 254 will be issued as necessary during the life of the contract when security requirements change.

e. A final DD Form 254 will be issued only if the contractor requests, in writing, an extension for classified material retention for an extended period after the contract period of performance.

f. The DD Form 254 shall be periodically reviewed during the performance stages of

the contract and a revised DD Form 254 will be issued if needed.

7. Common Access Card

a. Contractors who require access to the MCEN account must meet the minimum investigation requirement of NACI prior to Common Access Card (CAC) issuance.

b. When it has been determined that a contractor does not meet the minimum investigative requirements per reference (d), the government activity will ensure a Public Trust Positions Security Questionnaire, SF-85, is completed and provided to the SMO. The SMO will coordinate the remaining aspects of the investigation submission and fingerprinting.

c. Once the investigation questionnaire has been submitted to DCSA for processing and fingerprints and the results have returned favorably, the CAC will remain unrevoked. If the investigation does not return favorably, the CAC must be retrieved and revoked.

d. The contractors requiring CAC issuance only are assigned to a Trusted Agent. The eligibility and contracts carried by each contractor, along with their Trusted Agents, in this category is monitored by the Command Security Manager in the Trusted Associate Sponsorship System (TASS).

8. Check-Out/Debriefings. All contractors assigned to MCAS CHER PT must checkout with the SMO when leaving the Command.

a. Contractors who had access to classified information must be debriefed by the Command Security Manager.

b. Contractors will surrender all government issued property to the MCAS CHER PT SMO; such as DoD badges, CACs, and building access badges.

c. Contractors who have MCEN-S Tokens will surrender them directly to the MCAS CHER PT Telephone and Information Systems Directorate (TISD).

Chapter 7

Emergency Action Plans For Classified Material

1. General. This Emergency Action Plan (EAP) outlines instructions regarding actions to be taken to protect classified information and materials in the event of an emergency.

a. There are three types of emergencies that may arise. The first is natural disaster, which includes events such as fire, flood, tornado, earthquake, and lightning strike. Second are hostile actions such as sustained civil disturbances, insider threat, and terrorism. The third is casualty mishap, which includes collision, crash, or fire.

b. Actions to be taken during each type of emergency are distinctly different. Therefore, it is important that all authorized personnel have a thorough understanding of all potential emergencies and the action associated with each. The three options available are: securing the material, removing it from the scene, or destroying it. However, during the execution of any of these options, two person integrity (TPI) must be used during all execution steps.

c. Any significant activity (phone calls, message traffic, and events) relating to the destruction of classified material must be logged by all parties.

2. Courses of Action. When an emergency occurs, there are three courses of action possible for the protection of classified material.

a. Emergency Protection. If the situation dictates, classified material shall be stored in authorized containers. If feasible, an armed guard shall be posted near the containers. If the area is to be evacuated, a complete inventory shall be taken upon return to the area by authorized personnel to ensure no material is missing. The on-site Officer in Charge (OIC) will notate all pertinent information to include the full inventory in a memorandum of record.

b. Emergency Removal. If the situation dictates, it may become necessary for classified material to be removed.

(1) Emergency removal shall be conducted only when directed by the MCAS CHER PT Command Security Manager. The removal shall be under the complete and continuous supervision of the Command Security Manager.

(2) When supervised by the Command Security Manager, personnel without appropriate security clearances are able to assist. In the case of a fire, the removal shall not interfere with firefighting efforts or subject personnel to unnecessary danger.

(3) Removal of the material shall be coordinated in such a manner that the Command Security Manager knows the location of the material at all times.

(4) Transportation can be conducted via privately owned vehicle (POV), only if government transportation (GOV) is not available or it is deemed more efficient to transport the materials in this manner.

(5) The on-site OIC will ensure a thorough inventory during the transfer from the storage location to the GOV/POV and then from the GOV/POV to the new storage location. The on-site OIC will then conduct a thorough investigation of the GOV/POV to ensure no materials were left in the vehicle.

(6) During this transition, TPI must be utilized and must sign the inventory verification and be notated in the subsequent memorandum or record after the completion of the event.

(7) The relocation facilities are as follows:

(a) If another on base facility is necessary for temporary storage, the materials will be moved to MCIEAST's CMCC vault located in Bldg B1, Rm R134 or Bldg 60, Rm 161, the point of contact (POC) for these locations is the MCIEAST Command Security Manager.

(8) Some materials will require destruction rather than evacuation, the on-site OIC will work with the Command Security Manager to ensure all procedures are conducted appropriately.

c. Emergency Destruction. Emergency destruction actions include partial precautionary destruction and complete emergency destruction. When an emergency destruction situation is anticipated, it is highly desirable to first reduce the amount of classified information and material held to the minimum necessary to conduct essential operations. Destroying the material shall be conducted as the absolute last alternative. All reasonable efforts shall be made to secure or remove the material and place it in a secure location. In the unlikely event that emergency destruction is ordered, commence destruction in accordance with the priority listed below. A record of all material destroyed shall be maintained and provided to the senior person present upon completion of destruction. The following methods shall be used to destroy classified material:

(1) Shredding/Disintegration. Paper is only authorized for shredding on a National Security Agency (NSA) approved High-Security Cross-Cut Paper Shredder. Hard drives and other materials can be destroyed in NSA approved destruction equipment, located at MCAS CHER PT, rear of Bldg 151.

(2) Pulverization. Should the power be out, or should the shredding/disintegration machine be unavailable, the next course of action is to physically crush the materials to a reduction of fine particles. This is often used in situations where there is a power outage or NSA equipment is not accessible. The tool used for this process is a sledgehammer. Safety of the personnel performing the destruction is paramount, and eye protection is mandatory for this procedure.

(3) Burning. The very last course of action in CONUS, requires the on-site OIC must receive prior authorization from base environmental operations. However, during OCONUS

operation in accordance with the international and host nation agreements, burning may be utilized as a means of destruction. The individual assigned to destruction shall ensure that all documents are disassembled and crumpled individually. The material shall then be delivered to a designated area and burned in any appropriate receptacle and the on-site OIC must ensure there is considerable stand-off distance from personnel and other flammable objects such as vehicles, buildings, and the tree line. No liquid, such as gasoline, kerosene, or the like, will be used during the burn destruction procedures. A record of all material burned shall be maintained during destruction. All burn residue shall be thoroughly checked to ensure complete destruction as the situation dictates.

(4) Priorities of Destruction. In the case that destruction is the only means necessary to ensure safekeeping of materials and all other options have been exhausted, the priorities of destruction will be as follows:

(a) Top Secret

(b) Secret

(c) Confidential

(d) Non-essential classified manuals

(e) Any remaining material or equipment with operational or administrative data.

(5) TPI shall be enforced during drills and actual emergency destruction events involving classified equipment and materials.

(6) Accurate information relative to the extent of an emergency is absolutely essential to the effective evaluation of the COMSEC impact of the occurrence, and is second in importance only to the thorough destruction. State in the report the material destroyed, the method and extent of destruction, and any classified materials or items presumed compromised.

d. Emergency Destruction Responsibilities

(1) CO. The CO is overall responsible for all classified materials and information within the command's custody. He or she can authorize emergency destruction based on threat assessment and advisement of the Command Security Manager. Is responsible for reporting the attendant facts regarding any emergency destruction actions to the appropriate seniors in the chain of command by the most expeditious means available.

(2) Executive Officer (XO). The XO performs all emergency duties in the CO's absence.

(3) Command Security Manager. The Command Security Manager is responsible to the CO for all emergency destruction actions. This includes assessment, execution, and submission of required reports. He/she also advises the CO on threat conditions and emergencies, and is

responsible for destruction of all classified material. The Command Security Manager performs all emergency duties in the XO's absence.

e. Gaining Access to Secured Spaces. Each secured space has an X09 lock that guards the OSS space or the safe. Each X09 has SF700 documentation associated with the lock. The SF700 includes the combination and the instructions on how to use the lock. The SF700 for all spaces are located in AS-211, in the CMCC vault. In order to receive this combination, YOU MUST CONTACT THE COMMAND SECURITY MANAGER.

3. Emergency Situations

a. Fire. During a fire, if it is not possible to secure or remove classified materials, all items will be left in place to be consumed by the fire. UNDER NO CIRCUMSTANCES WILL ANYONE SUBJECT THEMSELVES OR THEIR SUBORDINATES TO POSSIBLE DEATH OR INJURY TO PROTECT THESE MATERIALS FROM A FIRE. The person(s) discovering the fire shall:

(1) Sound the alarm to notify others to immediately begin evacuation and fire safety procedures.

(2) Immediately notify the CO, XO, and the Command Security Manager. In the event all of these personnel are unavailable, the senior officer present will be designated the on-scene OIC. The on-scene OIC will maintain record of facts and critical information for reporting once these staff members have been contacted and located.

(3) The on-site OIC must notify local emergency responders by calling 9-1-1 if not already reported. All personnel shall familiarize themselves with the local emergency action reporting procedures, at a minimum, personnel calling must give building number and location of the fire and other details as requested by the emergency dispatch personnel.

(4) Take initial actions to contain and extinguish the fire if possible. Do not attempt to extinguish large or electrical fires that cannot be contained with the limited firefighting equipment in the vicinity.

(5) If time permits, secure as much classified material as possible in authorized security containers to prevent unauthorized viewing. Admit emergency personnel without delay. The Command Security Manager or on-scene OIC will maintain a watch of classified material at the storage location.

(6) When the fire is out and the area is secured, assess any possible exposure of classified materials and information to unauthorized personnel. If exposure is possible, obtain the names of all emergency response personnel granted access to restricted spaces and report to the Command Security Manager or on-site OIC and ensure all personnel sign a non-disclosure agreement (NDA).

(7) The on-site OIC must ensure a thorough inventory of all classified materials including COMSEC to determine what material was lost or damaged in the fire and submit a full report in the subsequent memorandum of record.

(8) Ensure a full report is given to the CO and the Command Security Manager as requested, or once the situation has been resolved.

b. Flood, Tornado, or Hurricane

(1) During a natural disaster, personal safety is paramount. UNDER NO CIRCUMSTANCES WILL ANYONE SUBJECT THEMSELVES OR THEIR SUBORDINATES TO POSSIBLE DEATH OR INJURY TO PROTECT THESE MATERIALS FROM A NATURAL DISASTER.

(2) If time permits, relocate all classified material and information to the most appropriate location as prescribed in section 2 above. If immediate emergency action is required, secure all classified materials and information in the normal storage containers and evacuate as directed.

(3) Some materials will require destruction rather than evacuation. The on-site OIC will work with the Command Security Manager to ensure all procedures are conducted appropriately.

(4) Immediately notify the CO, XO, and Command Security Manager. In the event all of these personnel are unavailable, the senior officer present will be designated the on-scene OIC. The on-scene OIC will maintain record of facts and critical information for reporting once these staff members have been contacted and located.

(5) When order is restored, return all classified materials to the authorized container. Assess any possible exposure of classified materials and information to unauthorized personnel. Obtain the names of all emergency response personnel granted access to restricted spaces and report to the Command Security Manager or on-site OIC and ensure all personnel sign an NDA.

(6) The on-site OIC must ensure a thorough inventory of all classified materials including Key Management Infrastructure (KMI) to determine what material was lost or damaged in the fire and submit a full report in the subsequent memorandum of record.

(7) As critical information is learned, the on-site OIC will brief the CO and XO with all pertinent facts surrounding the events and subsequent actions taken. The Command Security Manager will submit applicable reports required by directives.

c. Earthquake. Earthquakes occur unexpectedly and have the potential to damage structures and space integrity. As with other natural disasters, personal safety is paramount.

(1) If classified material is being utilized in a space with an authorized security container and securing the material to the nearest container would jeopardize personal safety, maintain custody of the material and proceed to safety.

(2) When safe to do so, immediately notify the CO, XO, and Command Security Manager. In the event all of these personnel are unavailable, the senior officer present will be designated the on-scene OIC and will take custody of the classified inventory, local destruction records, and other inventory documents.

(3) The on-scene OIC will maintain the record of facts and critical information for reporting once these staff members have been contacted and located.

(4) When order is restored, return all classified material to the authorized container. In the event structural damage prevents access to normal storage containers, store the material in the nearest authorized container and designate a 24 hour watch to guard the material.

(5) Admit emergency relief personnel to spaces as required, without delay. Assess any possible exposure of classified materials and information to unauthorized personnel. Obtain the names of all emergency response personnel granted access to restricted spaces and report to the Command Security Manager or on-site OIC and ensure all personnel sign an NDA.

(6) As critical information is learned, the on-site OIC will brief the CO and XO with all pertinent facts surrounding the events and subsequent actions taken. The Command Security Manager will submit applicable reports required by directives.

d. Rioting or Civil Uprising. It is unlikely that classified material and information is the target or desire during a civil uprising. These emergencies are usually politically and socially motivated and have little impact on military operations due to security measures in place.

(1) Immediately notify the CO, XO, and the Command Security Manager. In the event all of these personnel are unavailable, the senior officer present will be designated the on-scene OIC and will take custody of the classified materials.

(2) The on-scene OIC will maintain the record of facts and critical information for reporting once these staff members have been contacted and located.

(3) Ensure security containers are locked and all classified material is properly secured.

(4) If the situation warrants a destruction action, use precautionary or complete emergency destruction actions.

(5) As critical information is learned, the on-site OIC will brief the CO and XO with all pertinent facts surrounding the events and subsequent actions taken. The Command Security Manager will submit applicable reports required by directives.

e. Terrorist Attack. The first step is to determine the immediate threat to the compromise of classified materials and information. An assessment will be made through the Threat Assessment process and appropriate direction provided by cognizant authority.

(1) Immediately notify the CO, XO, and the Command Security Manager. In the event all of these personnel are unavailable, the senior officer present will be designated the on-scene OIC and will maintain record of facts and critical information for reporting once these staff members have been contacted and located.

(2) During terrorist attacks, the assumption must be made that classified materials and information is the target. Planning and action must be directed toward preventing authorized access to the material by hostile forces.

(3) If the threat is assessed as probable, imminent overrun, takeover of the facility, or other situation that warrants destruction action, implement Precautionary or Complete Emergency Destruction actions in Paragraph 2, subparagraph c, or as directed by a higher authority.

(4) As critical information is learned, the on-site OIC will brief the CO and XO with all pertinent facts surrounding the events and subsequent actions taken. The Command Security Manager or designated alternate will submit applicable reports required by directives.

f. Bomb Threat. In the event of a bomb threat, the on-site OIC will notify emergency services by dialing "9-1-1". Classified material will be secured immediately. All OSS spaces and safes will be locked and all classified material accounting records will be removed from the building. Personnel will wait outside the building at a safe distance until the arrival of local emergency responders. The building will not be re-entered until the "ALL CLEAR" signal is given by emergency response personnel or via the chain of command.

Chapter 8

Physical Security

1. General. As established in reference (j), MCAS CHER PT is required to provide physical safeguards for all Command personnel, information, and assets to deter from various undesirable events such as attacks, theft, sabotage, and espionage. These safeguards will be provided through various active and passive barriers, supplemental controls, and operating procedures. In all cases, implementation of these safeguards will be taken to ensure they are complementary to the installation safeguards and provide a layered approach to achieve security in-depth.

2. Responsibility

a. The Command Security Manager is responsible for compliance with and implementation of this Order.

b. The Command Security Manager is appointed as the Command Security Officer to ensure command compliance with Physical Security.

c. Program Managers and Supervisors are responsible for compliance with and implementation of this Order within their areas of responsibility.

3. Restricted Area Overview

a. Restricted Area (RA) Designation Types. There are three types of designation for restricted areas: Level One, Level Two, and Level Three. RA designation is often associated with areas storing classified information; however, there are other valid reasons to establish restricted areas to protect security interests.

(1) Level One. The least secure type of RA, it contains a security interest that if lost, stolen, compromised, or sabotaged would cause damage to the command's mission and national security. It may serve as a buffer zone for Level Three and Twos, providing access and administrative control, safety, and protection against sabotage, disruption, or potentially threating acts. Uncontrolled movement may or may not permit access to a security interest or asset.

(2) Level Two. The second most secure type of RA. It may be inside a Level One area, but will never be inside a Level Three. Level Two RAs contain a security interest that if lost, stolen, compromised, or sabotaged would cause serious damage to the command mission and national security. Uncontrolled or unescorted movement could permit access to the security interest or asset.

(3) Level Three. This Command does not maintain Level Three RAs.

b. Area Designation. RAs will be identified by the Command Security Manager and designated in writing annually and published with the Security and Emergency Services (SES) Physical Security, MCAS CHER PT.

c. Physical Security Survey (PSS). Surveys of RAs will be scheduled between SES Physical Security and the MCAS CHER PT Command Security Manager annually. SES Physical Security, MCAS CHER PT will coordinate the PSS with the departments and a representative will conduct the PSS.

d. Security POC. Each department shall identify in writing a primary and alternate security POC. These individuals will work directly with the SES Physical Security, MCAS CHER PT with scheduling a PSS and correcting issues with their department's RAs. These individuals may also be appointed as an Access Control Custodian.

4. Command's Restricted Areas. The CO, MCAS CHER PT has identified Station headquarters has assets within the following
list of all RAs within the command:

a. Level One. There are none.

b. Level Two

(1) Station Security/Mission Assurance Bldg HQ1, Room 1079

(2) METOC/Weather Bldg. 199, Room 113

(3) EOD Bldg 1795

(4) TISD Bldg 4397, Rooms 140 and 132

c. Level Three. There are none.

5. Storage Requirements

a. Classified information will only be stored in those areas which have been evaluated and approved, in writing, by the MCAS CHER PT Command Security Manager. Classified information will be stored in:

(1) A GSA-approved security container.

(2) A Class A or B vault.

(3) An approved secure room.

b. Security Containers. GSA establishes and publishes minimum standard, specifications, and supply schedules for security containers, vault doors, and modular vaults. Modification of any equipment used to store CNSI is prohibited. Contact the Command Security Manager for guidance on procurement of a GSA-approved security container or vault door.

c. Secure Rooms. A Secure Room is a cleared building, room, or space for open storage of classified information at the level designated by the MCAS CHER PT Command Security Manager. All Secure Rooms must meet the requirements of reference (a), Volume3, Appendix to enclosure (3) and will be designated in writing by the MCAS CHER PT Command Security Manager, and have a PSS conducted annually. If classified technologies are needed, contact MCAS CHER PT TISD.

(1) Only authorized cleared personnel will have access to secure rooms.

(2) All personnel who are not on the access roster to the designated secure rooms are considered visitors and will utilize the visitor log, to include maintenance personnel. At all times while in the secure room all visitors will be escorted by an authorized person.

(3) Each secure room will have a designated point of contact who works directly with the MCAS CHER PT Command Security Manager in the management of the space.

(4) In the event of an emergency, law enforcement and emergency personnel are authorized access to all designated MCAS CHER PT secure rooms. After access is no longer required, immediately notify the MCAS CHER PT Command Security Manager. The Command Security Manager will handle all follow-on procedures. These procedures may include, but are not limited to, inadvertent disclosure briefs and execution of a SF-312 and debrief forms.

d. Combination Locks

(1) Combinations to security containers will be changed only by trained individuals having the responsibility and appropriate security clearance. The MCAS CHER PT Command Security Manager will provide required training to designated personnel.

(2) The combination will be given only to authorized personnel whose official duties require access to the container or space.

(3) Combinations will be changed when containers/locks are first placed in use and when any of the following occurs:

(a) An individual knowing the combination no longer requires access.

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

(c) The container is taken out of service.

(4) The SF-700 will be used to record combination changes. The SF-700 is a form that contains vital information about the security container in which it is located. This information includes location, container number, lock serial number, and contact information if the

container is found open and unattended. The SF-700 will list the personnel who have access to the combination and the detachable portion of the combination envelope will be attached inside the locking drawer. The MCAS CHER PT Command Security Manager will maintain Part II of all executed SF-700s throughout the command. Personnel with access to the combinations must have eligibility and access granted equal to the classification of the combinations. Part II of the SF-700 will be classified at the same level of material it protects. Part I of the SF-700 will be marked CUI. The SF-700 shall be destroyed once replaced by a new SF-700.

(5) Repairs To Damaged Security Containers. A school trained locksmith is authorized to repair and replace parts on all security equipment and should be called upon when required. The MCAS CHER PT Command Security Manager and MCAS CHER PT Installation and Environmental Department will be responsible for contracting a locksmith to make necessary repairs and will pay for such repairs. Under no circumstances will repairs be made or attempted by untrained personnel. All repairs or modifications must be recorded on an Optional Form 89. A properly cleared individual will be present at all times when maintenance is performed on security containers storing classified material.

6. Security Checks and End of the Day Checks

a. Classified RAs. All Restricted Access Areas (RAAs), Controlled Access Areas (CAAs), and Secure Rooms must use the SF-701, Activity Security Checklist, to record security checks at the close of each duty and/or business day to ensure the area where classified information is used or stored is secure. An integral part of the security check will be the securing of all vaults, secure rooms, and containers used in storing classified information. The SF-702, Security Container Check Sheet, will be used to record such actions. The SF-701 and SF-702 shall be maintained for 60 days after date of last security check.

b. After-Hours Checks. After-hours checks will be conducted by the CDO and must be checked every four hours and annotated on the SF-702s for the following classified spaces. During weekends and holidays, these areas will be inspected every four hours throughout the CDO's tour of duty.

(1) Station Security/Mission Assurance Bldg HQ1, Room 1079

c. Non-Classified RAs. All other non-classified, but designated RAs, shall use the SF-701, Activity Security Checklist, to record security checks at the close of each duty and/or business day to ensure the areas are secure. The CDO shall also conduct after-hours checks to ensure these remain secure and annotate the security checks in the CDO Log Book. The CDO shall inspect the following location at least once after 1630 during work days, and at least twice during non-work days such as weekends and holidays.

(1) METOC/Weather Bldg. 199

(2) EOD Bldg 1795 (exterior of fenced perimeter)

(3) TISD Bldg 4397

7. Access Control. The access control and key program will be supervised by the Access Control Officer (ACO). Included in this program are all keys, locks, padlocks, and locking devices used to secure RAs, activity perimeters, security facilities, critical assets, sensitive material, and supplies per the unit's Designation of RA letter. Not included in this program are keys, locks, and padlocks for convenience, privacy, unclassified administrative or personal use.

a. Access Rosters. Access rosters shall be completed for all personnel with unescorted access to RAs. OICs may sign these rosters for non-classified RAs. The Command Security Manager will sign for all classified spaces.

8. Signs and Posting of Boundaries. Perimeter barriers of all RAs will be posted with signs measuring approximately 12 inches by 18 inches in size with proportionate lettering. Signs will read as follows:

WARNING
RESTRICTED AREA
KEEP OUT
AUTHORIZED PERSONNEL ONLY

a. All barrier signs will be placed so as not to obscure the necessary lines of vision for security force personnel.

b. Color Code. All signs shall be color coded to provide legibility from a distance of at least 100 feet during daylight hours under normal conditions. The following color codes are recommended restricted/non-RA perimeter signs:

(1) All words except WARNING will be black.

(2) The word WARNING will be red.

(3) All wording will be on white backgrounds to obtain maximum color contrast.

c. Signs will be properly maintained. Defective and faded signs will be replaced.

d. These signs may be contracted for or produced locally at the command.

9. Protected Distribution Systems Inspections (PDS). The PDS daily visual inspections log and the PDS annual technical inspections checklist will be conducted per the below procedures, and in accordance with references (e) and (f).

a. Daily Visual Inspections

(1) Daily visual inspections of the PDS are required. These inspections will be conducted by authorized personnel designated by the MCAS CHER PT Command Security Manager. The Command Security Manager will ensure personnel are properly trained to inspect the PDS and

able to identify signs of tampering, breakage, or unserviceability per reference (e). The authorized personnel are responsible to visually inspect the following PDS locks:

(a) Bldg HQ1, Room 1127, lock 653245

(b) Bldg HQ1, Room 1225, lock 234073

(c) Bldg HQ1, Room 1121, lock 632177

(d) Bldg HQ1, Room 1118, lock 433592

(e) Bldg HQ1, Room 1092, lock 432779

(f) Bldg HQ1, Room 1093, lock 432762

(g) Bldg HQ1, Room 2112, lock 657811

(h) Bldg HQ1, Room 2132, lock 662648

(2) Visually inspect the PDS conduit carefully along its entire pathway looking for signs of tampering, breakage, or unserviceability. Signs of tampering include tool marks, conduit loosened from stand-offs, discolored conduit, or deviation from the PDS diagram. Look for devices or material added to or against the PDS (material against the PDS can conceal signs of tampering).

(3) Give particular attention to conduit joints (epoxy sealed joints), pull-boxes, and drop-boxes. Look for tool marks, chipped or discolored epoxy, or an epoxy joint that looks different than the others. Ensure pull-boxes and drop-boxes are secured with an S&G combination padlock. Look for signs of tampering of the locks or pull-box and drop-box covers. Look for signs of tool marks, chipped paint, or box covers not sealed flat against the box. Drop-cables (cables from drop-box to computer) shall not remain connected to unattended drop-boxes. Drop-cables shall be stored in the drop-box or GSA approved container.

(4) If signs of tampering, breakage, or any other anomalies are identified, post a guard immediately on the affected site and immediately contact the Command Security Manager. Do not disturb or advertise the finding; maintain a need-to-know posture. The Command Security Manager can be reached at (252) 466-6557. The Command Security Manager will investigate and report on the finding. If it does not look right or was not there the day before, report it.

(5) If the room is secured, ensure the door or doors have not been tampered with. Check the door for signs of tampering.

(6) Upon completion of the visual inspection, make an entry on the SF-702 and in the CDO/ADO logbook.

b. Annual Technical Inspections. The PDS annual technical inspection checklist, will be conducted once per calendar year by a USMC Authorizing Officer (AO) appointed PDS

inspector, in accordance with this procedure and reference (e). The Command Security Manager will coordinate with the local PDS inspector to schedule the inspection. The annual inspection will follow similar procedures of the daily inspections but in a hands-on, hand-over-hand approach.

c. PDS and Terminal Area Modifications. Any proposed modifications to the PDS or terminal areas as certified shall be coordinated with the ISSM. The MCAS CHER PT TISD, in coordination with the Command Security Manager shall complete the updated PDS design approval request (PDAR) and forward by email to the MCIEAST G-6 Assessment and Authorization for review and approval.