



UNITED STATES MARINE CORPS  
2D MARINE AIRCRAFT WING  
II MARINE EXPEDITIONARY FORCE  
POSTAL SERVICE CENTER BOX 8050  
CHERRY POINT, NC 28533-0050

5510  
SecMgr  
AUG 27 2012

POLICY LETTER 01-12

From: Commanding General, 2d Marine Aircraft Wing  
To: Distribution List

Subj: INTERNAL SECURITY PROCEDURES FOR 2D MARINE AIRCRAFT WING  
HEADQUARTERS (2D MAW HQ)

Ref: (a) SECNAV M-5510.30  
(b) SECNAV M-5510.36  
(c) MCO 5510.14A  
(d) WgO 5510.1T

Encl: (1) SF 701 Activity Security Checklist  
(2) SF 702 Security Container Check Sheet  
(3) Classified Material Cover Sheets (SF 705/704/703)  
(4) Diagram of Building 1  
(5) 2d MAW Security Badges  
(6) II Marine Expeditionary Force (II MEF) Reciprocity  
Badge Agreement  
(7) Marine Corps Air Station (MCAS) Reciprocity Badge  
Agreement

1. Purpose. In accordance with the references, appropriate security procedures must be followed in order to prevent disclosure of classified material to unauthorized personnel. 2d MAW HQ is defined as G-1, G-2, G-3, G-4, G-5, G-6, Staff Secretary (SSEC), Wing Inspector General (IG), Aviation Logistics Department (ALD), Wing Medical, Wing Chaplain, Wing Comptroller, Staff Judge Advocate (SJA), Wing Safety, Marine Aviation Training Systems Site (MATSS) and Marine Wing Headquarters Squadron 2.

2. Background. To ensure adequate security measures are taken, the following procedures are established:

a. Sections of the 2d MAW HQ are responsible for safeguarding all classified material within their respective

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

Subj: INTERNAL SECURITY PROCEDURES FOR 2D MARINE AIRCRAFT WING  
HEADQUARTERS (2D MAW HQ)

section. It is the responsibility of all 2d MAW HQ personnel to ensure classified material is properly safeguarded at all times.

b. Classified materials will be handled in the manner prescribed in reference (b) for the level of classified information they contain. Examples of classified materials include computer hard drives, CDs, binders, documents, email, maps, briefings (to include PowerPoint presentations), etc.

c. All Personal Electronic Devices (PEDs) are not authorized in open storage areas. This includes vaults, secured rooms or any other area where the primary type of data being processed, stored or discussed is classified (MARADMIN 375/01).

d. The 2d MAW Security Manager will be the Access Control Officer for 2d MAW HQ. A duplicate of all keys and combinations to workspaces and secure areas will be maintained and controlled by the 2d MAW Security Manager.

3. Policy. Upon check-in, all personnel assigned to the 2d MAW HQ will receive a designated security badge. Whenever the individual transfers away from 2d MAW HQ he/she will return his/her security badge to 2d MAW Security Office. All 2d MAW HQ personnel and visitors are required to wear their security badge when inside of Building 1 (Bldg 1). Enclosure (5) identifies 2d MAW security badges. II Marine Expeditionary Force (II MEF) and Marine Corps Air Station (MCAS) Cherry Point Security Manager have approved reciprocal badge validation and acceptance with 2d MAW (See enclosure (6) and (7)).

a. 2d MAW HQ Sections will ensure all access documentation is filled out daily. This includes:

(1) The Activity Security Checklist Standard Form (SF 701, enclosure (1)). Sections must ensure this form is completed daily and is posted on the inside of the main entrance door the respective section.

(2) The Security Container Check Sheet (SF 702, enclosure (2)). Sections must ensure this form is attached to all security containers, vaults and safes and is completed daily.

b. When classified material is handled, processed or transferred sections must ensure:

Subj: INTERNAL SECURITY PROCEDURES FOR 2D MARINE AIRCRAFT WING HEADQUARTERS (2D MAW HQ)

(1) Classified materials are properly marked; documents, folders, binders and briefings have a cover sheet (SF 704, 705 (enclosure (3)) attached. Electronic Classified Material (Computers, hard drives, CDs etc.) is properly marked with the appropriate classification, using color codes and SF 700 series stickers.

(2) All classified correspondence inboxes are properly marked for holding classified materials. This will prevent the inadvertent intermingling of classified materials with unclassified materials.

(3) Classified materials are properly secured at the end of day and when leaving the immediate area. Classified material will not be left unattended for any reason.

c. The transportation of classified material out of designated work spaces is approved by the 2d MAW Security Manager.

d. All 2d MAW personnel entering and exiting Bldg 1 must use the back lobby entrance except for personnel who are authorized access through the ceremonial entrance. All other doors of Bldg 1 are for emergency exit use only.

e. In accordance with reference (b), anyone working after normal working hours (0530-1730 Monday through Friday), weekends and holidays will ensure:

(1) He/she checks in and out with the Command Duty Officer (CDO).

(2) Access to all workspaces (e.g. vaults, secure rooms, security containers and safes) is properly documented and secured. This includes the requisite documentation on the SF 702 and the SF 701 at the conclusion of the work day.

f. All classified material is accounted for by the Classified Material Control Center (CMCC). The only exceptions are working papers that have less than 180 days since their original creation. All working papers passing the 180 day limit must be turned in to the CMCC for control and accountability. All transfer or destruction of classified material, to or from a section, must be coordinated with the CMCC.

Subj: INTERNAL SECURITY PROCEDURES FOR 2D MARINE AIRCRAFT WING HEADQUARTERS (2D MAW HQ)

g. In closed storage areas, Secure Telephone Equipment (STE KOV-14) crypto cards must be secured at the end of day or when the workspace is left unattended.

4. Procedures used to ensure the security of the Secret Internet Protocol Router Network (SIPRNET):

a. All SIPRNET users must have a minimum of an Interim Secret clearance and a "need-to-know" to access the SIPRNET.

b. While utilizing SIPRNET the user will ensure the area is secure. This includes closing the window blinds and locking the dead-bolt on all doors leading to the room in closed storage areas.

c. Users will not leave SIPRNET computers unattended in any area that is not approved for open storage.

d. Ensure IT maintenance personnel from outside the unit are properly identified before they begin work on any SIPRNET information system. These individuals should be escorted and continuously monitored during maintenance. If an individual does not have proper identification and their credentials cannot be confirmed, do not allow them access to controlled areas.

e. In closed storage areas, ensure each Protective Distribution Systems (PDS) box has an SF 702 (enclosure(2) attached to the box or wall. This form must be filled out daily and each time the box is opened or secured.

5. Guidelines for Visitors

a. A visitor is defined as any personnel not belonging to 2d MAW HQ.

b. All 2d MAW HQ visitors must check in and out with the 2d MAW Security Management Office when entering and leaving Bldg 1 or the CDO for after-hours. (Note: this does not apply to MCAS personnel who work inside of Bldg 1 and have a Station Badge).

c. All visitors are subject to search upon entering and leaving the building.

d. Visitors will be escorted at all times in classified and unclassified workspaces.

Subj: INTERNAL SECURITY PROCEDURES FOR 2D MARINE AIRCRAFT WING  
HEADQUARTERS (2D MAW HQ)

e. All sections must verify a visitor's clearance via Joint Personnel Adjudication System (JPAS) before allowing access to classified areas or materials.

6. CDO Guidelines. CDO must tour the inside building twice during the week days and three time during weekend/holidays, to ensure no tampering or unauthorized attempts to enter the building have occurred.

a. During the CDO tour she/he is required to check off on all SF 702 forms (See enclosure (2)) in the following workspaces(See enclosure (4)) ALD, rooms 1032, 1033, 1035,G-2, rooms 2020B, 2021, G-3, rooms 2020C, 2053, G-4, room 2122, G-6, rooms 1020, 2068, 2069, 2070, 2074 and the Security Management room 2018.

b. In the event of a security breach or concern, the CDO will contact the 2d MAW Security Manager at (252) 876-6308.

7. For further assistance or clarification in implementing these procedures contact Marcus Allen, 2d MAW Security Manager at (252) 466-6071/7464; or Non-Secure Internet Protocol Router (NIPRNET) e-mail [marcus.1.allen@usmc.mil](mailto:marcus.1.allen@usmc.mil).

8. Filing Instructions. A copy of this policy shall be maintained on file.

  
G. M. WALTERS

DISTRIBUTION: A

# ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE

2D MAW SECURITY OFFICE

ROOM NUMBER

Bldg 1

MONTH AND YEAR

Oct 2011

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all items listed below.

TO (if required)

THROUGH (if required)

FROM (if required)

2D MAW SECURITY MANAGER

ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. All classified material secured																															
2. Security containers have been locked and checked.																															
3. Safe locked, SF 702 Container (double check)																															
4. Personnel files locked; key secured																															
5. NIPR/SIPR logged off																															
6. PCs, copiers, coffee pot, and radios turned off																															
7. Windows Shut/Locked																															
8. Lights off/Door locked																															
9. SF 701 Activity Security Checklist Completed																															
INITIAL FOR DAILY REPORT																															
TIME																															



# **CONFIDENTIAL**

**THIS IS A COVER SHEET**

**FOR CLASSIFIED INFORMATION**

**ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.**

**HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.**

**(This cover sheet is unclassified.)**

# **CONFIDENTIAL**

705-101  
NSN 7540-01-213-7903

**STANDARD FORM 705 (8-85)**  
Prescribed by GSA/ISOO  
32 CFR 2003

# SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT MUST BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

# SECRET

704-101  
NSN 7540-01-213-7902

STANDARD FORM 704 (8-85)  
Prescribed by GSA/ISOO  
32 CFR 2003

# TOP SECRET

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT WILL BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

# TOP SECRET

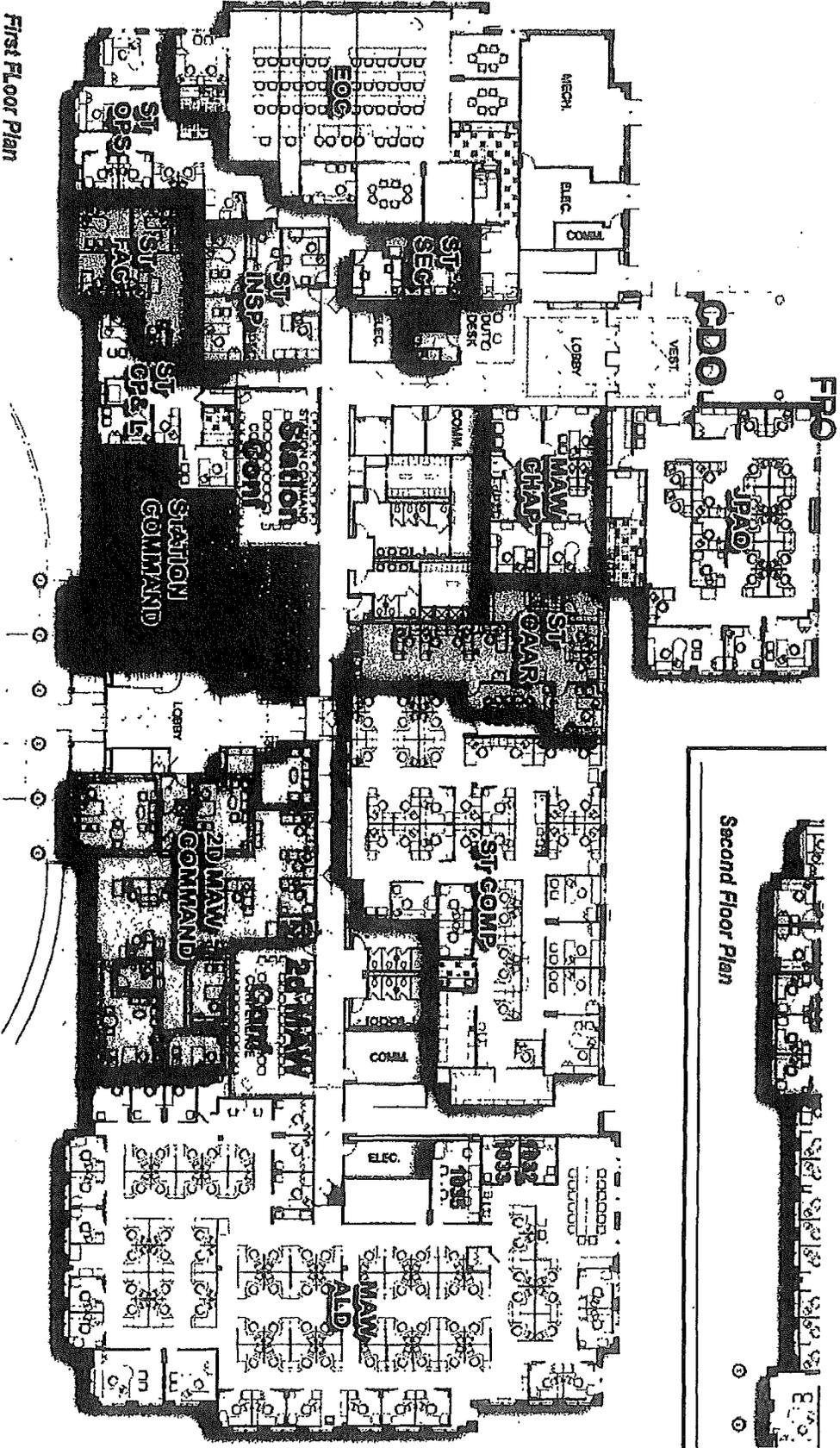
703-101  
NSN 7540-01-213-7901

STANDARD FORM 703 (8-85)  
Prescribed by GSA/ISOO  
32 CFR 2003

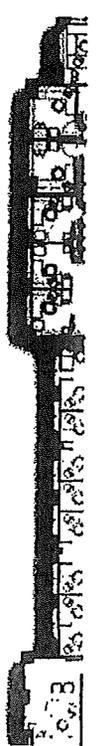
# First Floor Utilization

## 2d MAV

First Floor Plan



Second Floor Plan



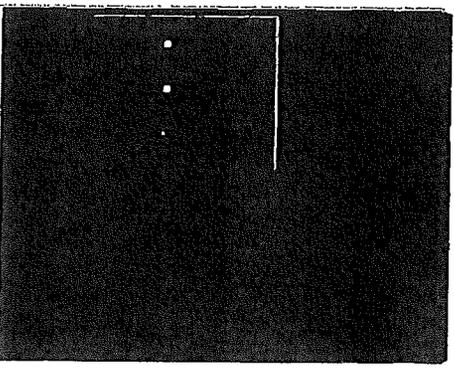




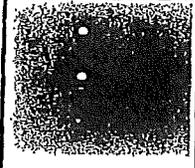
This Credential is property of the United States Government. Its counterfeiting, alteration, or misuse is a violation of 18 USC Section 499. It shall be returned to the issuing office upon termination or demand.

If found return to:  
 Commanding General  
 ATTN: 2D MAW Security  
 Manager  
 PSC Box 8076  
 MCAS CHERRY POINT, NC  
 28533-0076  
 PH#: 252-466-6071

Badge Issued By:  
*Marcus L. Allen*



2D MARINE AIRCRAFT WING



DOE, JOHN L  
 CTR USA  
 0000559  
 Expires  
 17 Nov 2012

If found return to:  
 COMMANDING GENERAL  
 ATTN: 2D MAW SECURITY  
 MANAGEMENT  
 PSC BOX 8076  
 MCAS CHERRY POINT, NC  
 28533-0076  
 PH#: 252-466-6071/7464

Badge Issued By:  
*Marcus L. Allen*

**2D MAW BADGE IDENTIFICATION**  
 The front side of this badge has the individual photo, name, rank, country, badge number and expiration date. White with no number identifies that the individual has not been granted US Access. Backside of the badge has the 2d MAW Security Office contact information.



This Credential is property of the United States Government. Its counterfeiting, alteration, or misuse is a violation of 18 USC Section 499. It shall be returned to the issuing office upon termination or demand.

If found return to:  
 Commanding General  
 ATTN: 2D MAW Security  
 Manager  
 PSC Box 8076  
 MCAS CHERRY POINT, NC  
 28533-0076  
 PH#: 252-466-6071

Badge Issued By:  
*Marcus L. Allen*

2D MARINE AIRCRAFT WING

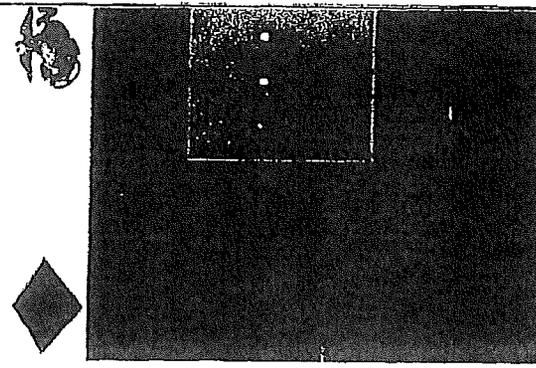
3

DOE, JOHN L  
 CTR USA  
 0000559  
 Expires  
 17 Nov 2012

This Credential is property of the United States Government. Its counterfeiting, alteration, or misuse is a violation of 18 USC Section 499. It shall be returned to the issuing office upon termination or demand.

If found return to:  
 Commanding General  
 ATTN: 2D MAW Security  
 Manager  
 PSC Box 8076  
 MCAS CHERRY POINT, NC  
 28533-0076  
 PH#: 252-466-6071

Badge Issued By:  
*Marcus L. Allen*



**2D MAW BADGE IDENTIFICATION**

The front side of this badge has the individual photo, name, rank, country, badge number and expiration date. Yellow with the number three identifies that the individual has top secret eligibility and has been granted SCI Access. Backside of the badge has the 2d MAW Security Office contact information.



UNITED STATES MARINE CORPS  
II MARINE EXPEDITIONARY FORCE  
PSC BOX 20080  
CAMP LEJEUNE, NC 28542-0080

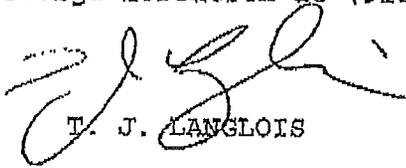
IN REPLY REFER TO:  
5510  
MPWR  
5 Dec 11

From: Security Manager, II Marine Expeditionary Force  
To: Security Manager, 2d Marine Aircraft Wing

Subj: RECIPROCATORY BADGE AGREEMENT BETWEEN II MARINE  
EXPEDITIONARY FORCE, CAMP LEJEUNE AND 2D MARINE AIRCRAFT  
WING, CHERRY POINT

Ref: (a) 2D MAW ltr 5510 SecMgr of 29 Nov 11

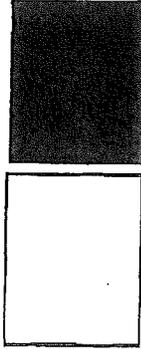
1. In accordance with the reference, the II Marine Expeditionary Force Security Manager has approved reciprocal badge validation and acceptance with 2d Marine Aircraft Wing.
2. Security Manager, 2d Marine Corps Aircraft Wing will screen and issue all personnel badges numbered and color coded per the reference. All other procedures agreed upon are accepted.
3. Point of contact is Mr. George Lorentson at (910) 451-5393.

  
T. J. LANGLOIS

Encl: 6 (1)



II MARINE EXPEDITIONARY FORCE



John Doe  
II MEF TOP SECRET

II MEF BADGE IDENTIFICATION

Top Secret Access



II MARINE EXPEDITIONARY FORCE



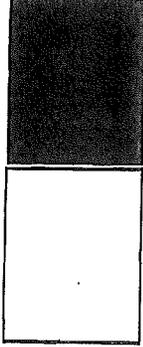
John Doe  
II MEF SECRET

II MEF BADGE IDENTIFICATION

Secret Access



II MARINE EXPEDITIONARY FORCE



John Doe  
II MEF UNCLAS

II MEF BADGE IDENTIFICATION

No Access



UNITED STATES MARINE CORPS

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

IN REPLY REFER TO:

5510

MPWR

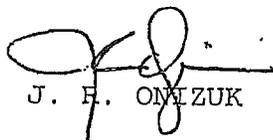
30 Nov 11

From: Security Manager, Marine Corps Air Station, Cherry Point  
To: Security Manager, 2d Marine Aircraft Wing

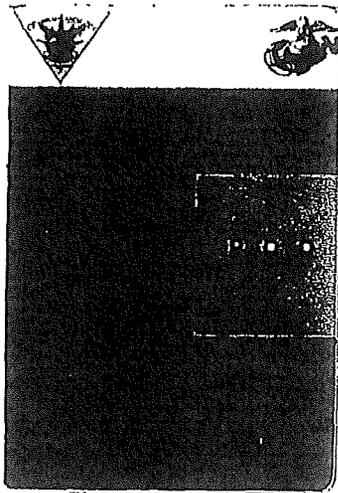
Subj: RECIPROCATORY BADGE AGREEMENT BETWEEN 2D MARINE AIRCRAFT  
WING AND MARINE CORPS AIR STATION CHERRY POINT

Ref: (a) 2D MAW ltr 5510 SecMgr of 29 Nov 11

1. In accordance with the reference request in paragraph 4, Marine Corps Air Station, Cherry Point approves reciprocal badge validation acceptance.
2. Security Manager, Marine Corps Air Station, Cherry Point will screen and issue all personnel in Building 1 badges numbered and color coded per the reference. All other procedures agreed upon are accepted.
3. Point of contact is Mr. Joe Onizuk at 466-3913.

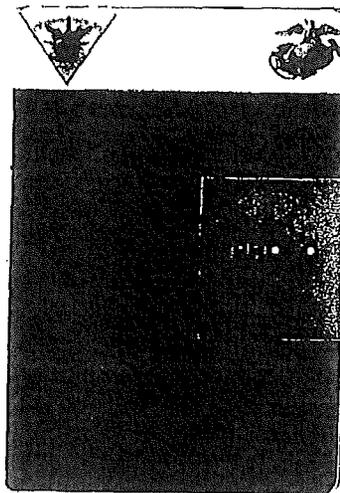
  
J. H. ONIZUK

Encl: 7(1)



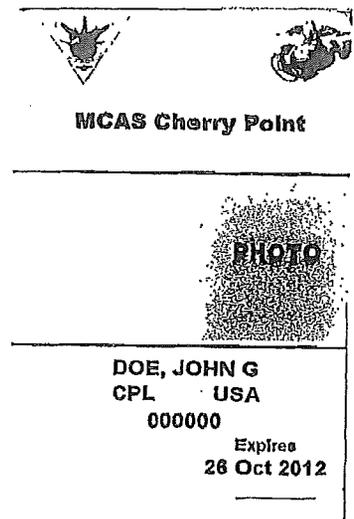
**MCAS BADGE**  
**IDENTIFICATION**

**Top Secret Access**



**MCAS BADGE**  
**IDENTIFICATION**

**Secret Access**



**MCAS BADGE**  
**IDENTIFICATION**

**No Access**