



DEPARTMENT OF THE NAVY

COMMANDER,
NAVY REGION MID-ATLANTIC
1510 GILBERT STREET
NORFOLK, VA 23511-2737

IN REPLY REFER TO:
COMNAVREGMIDLANTINST 5530.14A
N3

31 MAR 2014

COMNAVREG MIDLANT INSTRUCTION 5530.14A

From: Commander, Navy Region Mid-Atlantic

Subj: MID-ATLANTIC REGION INSTALLATION ACCESS CONTROL PROGRAM

Ref: (a) DoD DTM 09-012
(b) DoDI 1000.13
(c) DoDI 2000.16
(d) SECNAV M-5210.1
(e) OPNAVINST 5530.14E
(f) CNICINST 5530.14A
(g) OPNAVINST 1752.3
(h) BUPERSINST 1750.10
(i) DoD 5200.08-R
(j) DoDI 5200.08
(k) DoDD 2000.12 - AT Program
(l) COMUSFLTFORCOM OPOD 3300 (Series)
(m) DoD O-2000.12-H - AT Handbook
(n) SECNAV memo of 7 Oct 08
(o) SECNAV M-2510.1
(p) USFF Force Protection (FP) Directive 11-009
(111900Z MAY 11)

Encl: (1) Commander, Navy Region Mid-Atlantic Installation
Access Control Program Guidance
(2) Access Control for Senior Officer Functions
(3) Special Event Antiterrorism Plan (SEAT) Guidance
(4) Seat Decision Flow Chart
(5) Sample SEAT submission Template - On Base (Large)
(6) Sample SEAT submission Template - Off Base
(7) Sample SEAT submission Template - On Base (Small)

1. Purpose. Provide and promulgate standardized installation access control policy and guidance for Commander, Navy Region Mid-Atlantic (CNRMA), in accordance with (IAW) references (a) through (p).

2. Cancellation. COMNAVREGMIDLANTINST 5530.14.

31 MAR 2014

2. Cancellation. COMNAVREGMIDLANTINST 5530.14.

3. Background

a. Scope. This instruction defines the responsibility of Installation Commanders and Commanding Officers (CO) (both are hereafter referred to as 'CO') in establishing, implementing, and sustaining scalable Base Operating Support (BOS) related access control procedures. These procedures are based on guidance from Commander, U.S. Fleet Forces Command (COMUSFLTFORCOM) and Commander, Navy Installations Command (CNIC) Required Operational Capability (ROC) Levels and Force Protection Conditions (FPCON).

b. Exemption. This instruction does not address mission-related access control areas and their specific procedures and capabilities.

c. Applicability. This instruction applies to all Navy installations within the CNRMA area of responsibility (AOR). This instruction is applicable to DoD personnel, including active and reserve components, DoD civilians, DoD families, Navy and non-Navy tenants, contractor personnel, visitors, guests, and foreign national personnel.

4. Policy. In accordance with references (a) through (n), the primary objectives of the CNRMA Access Control Program are as follows:

a. Protect personnel and critical operational assets on board Navy installations.

b. Standardize and integrate identification, authorization, authentication, credentialing, and access.

c. Establish minimum access standards for all UNESCORTED persons. All unescorted persons must:

- (1) Have a valid purpose to enter
- (2) Be identity-proofed
- (3) Have identity-vetted
- (4) Possess a valid access credential

d. Establish/Validate requesting personnel's background utilizing the following methods:

31 MAR 2014

- (1) The National Crime Information Center (NCIC) Database
- (2) The Terrorist Screening Database
- (3) The Sex Offender Registry & Notification Act (SORNA)
- (4) The Foreign Visitor System - Confirmation Module
(FVS-CM)
- (5) The Department of Homeland Security (E-Verify)
- (6) The Department of Homeland Security (U.S. VISIT)
- (7) The Department of State Consular Checks (non-U.S. citizen)

e. In order to safeguard Personally Identifiable Information (PII), all PII collected and utilized in execution of background checks is protected to prevent any unauthorized use, disclosure, and or loss, per reference (o).

5. Access Authorization and Requirements. Access to Navy installations is not a right, and is within the Installation CO's discretion when complying with established policies and procedures. Effective security cannot be achieved by relying solely on the effectiveness of the sentry at the Entry Control Point (ECP). An integrated and synchronized approach is required to ensure all persons entering the installation have a justified reason for access and proper vetting has occurred. Installation COs should also address and control access at off-installation facilities in accordance with their Anti-terrorism (AT) plan. At a minimum, consideration should be given to threat, criticality, and vulnerability in the risk assessment process.

a. All unescorted persons entering CNRMA installations must have a valid purpose to enter, must be identity-proofed and vetted, and be issued, or in possession of, an authorized and valid access credential. Escorted personnel do not have the same background check requirements. Special events that are covered under an AT plan (e.g., Force Protection Special Event (FPSE), Air Show, Change of Command) do not need to meet the vetting process of this instruction. FPSE AT plans must address non-vetted and unescorted person controls and mitigating factors.

b. The following personnel are authorized unescorted access and need no further vetting. Additionally, these personnel can serve as Escort/Trusted Traveler/Sponsor for installation access

31 MAR 2014

during FPCON Normal, Alpha, Bravo, and as detailed in the installations AT plan.

Active Duty	CAC ID
Reserve	CAC ID
Dependents (age 16 or older)	Military ID
Military Retirees	Military ID
Civil Service Employees	CAC ID

c. Vetting of the above personnel is accomplished as follows:

(1) Department of Defense (DoD) Military Personnel are vetted with a National Agency Check for Law and Credit and, when in possession of a CAC Identification (ID), have met the requirements of paragraph 3.

(2) A DoD Civilian Personnel National Agency Check with Inquiries (NACI) and, when in possession of a CAC ID, have met the requirements of paragraph 3.

(3) Per reference (a), determination of fitness and vetting for DoD-issued ID and privilege cards (Dependent ID Card) is not required for unescorted access. The issuing office verifies the individual's direct affiliation with DoD, or a specific DoD sponsor, and eligibility for DoD benefits and entitlements.

(4) Persons possessing a DoD-issued card IAW reference (b) are identity-proofed at card issuance sites from federally authorized identity documents, and shall be considered identity-proofed.

NOTE: Contractors are not authorized to serve as Escorts, Trusted Traveler, or Sponsors.

6. Gold Star Family Members

a. Blue and Gold Star service banners have been in existence since World War I. The American Legion rekindled the spirit of pride in our military men and women following the September 11, 2001 terrorist attacks.

b. The blue star represents one family member serving, and a banner may have up to five stars. A Gold Star indicates that a loved one has been lost in war.

31 MAR 2014

c. The Army has expanded this tradition further by issuing Gold Star Family members a special decal along with special installation access cards allowing them access to Army installations. CNIC does not accept these cards or decals to access any CNIC installations or facilities.

d. The policy for NSF members is to know what a "gold Star" family member is and afford them the respect that should be accorded to someone who has lost a loved one in the defense of our country.

e. Gold/Blue star personnel requesting access to CNRMA installations will be granted access after successfully meeting the requirements listed in paragraph 4.

7. Assumptions

a. The Navy Commercial Access Control System (NCACS) and day visitor passes, will be the primary access control system for contractors and vendors who are not authorized Command Access Cards. Vetting for NCACS participants will occur every 92 days, and for day visitors, every 90 days. Additionally, nonparticipants must receive an installation pass daily.

b. Access capability is situation-dependant based on FPCON.

c. Manpower requirements will be commensurate with ROC level and threat conditions.

8. Responsibilities. All CNRMA installations will incorporate access control procedures required by the CNRMA installation Access Control Program.

a. Commander, Navy Region Mid-Atlantic shall:

(1) Have overall responsibility for establishing guidance related to CNRMA installation access control.

(2) Develop and promulgate access control guidance based on the standards set forth in references (a) through (o).

b. Installation COs within the CNRMA AOR:

(1) Are granted the authority and responsibility to protect personnel, equipment, and facilities subject to their control. Neither this instruction nor the access control program

31 MAR 2014

shall detract from, or conflict with, the inherent and specified authorities and responsibilities of the Installation CO.

(2) Shall implement the CNRMA Access Control Program as detailed within enclosure (1).

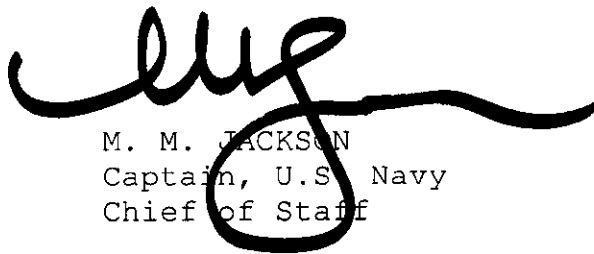
(3) Will integrate guidance and standards provided in enclosure (1) into local installation FP planning.

(4) Will conduct random vehicle and personnel inspections as part of Random AT Measures (RAM) IAW reference (c).

(5) Will ensure resources and manpower are not expended on the development of local access control databases, credentialing systems, and associated badges without prior coordination with the Naval Facilities Engineering Command (NAVFAC) AT/FP Program Manager and the Region Public Safety Program Director (Region N3).

(6) Are authorized to conduct random proofing and vetting of persons requiring access to their assigned installations, as necessary and appropriate.

9. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed IAW reference (o).



M. M. JACKSON
Captain, U.S. Navy
Chief of Staff

Distribution: Electronic only, via CNIC GATEWAY PORTAL, Region Sites, <https://g2.cnic.navy.mil/CNRMA/Pages/Default.aspx>

31 MAR 2014

Commander, Navy Region Mid-Atlantic Installation
Access Control Program Guidance

1. Overview: Guidance defined in this section shall be used to develop a comprehensive installation personnel access control program. This instruction does not address movement control. These capabilities should be considered dynamic and, as such, will be reviewed on a regular basis.

a. Installations shall develop a comprehensive personnel and vehicle access, identification, and movement control system that provides a visible means to identify and account for personnel and vehicles authorized access to Naval installations. Installation COs shall establish a process for removal of, or denying access to, persons who are not authorized or represent a criminal threat IAW the sensitivity, classification, value, or operational importance of the installation and the requirements of this instruction. The Installation CO has the authority to alter and enforce additional access control policy measures during elevated FPCONs and emergent situations to protect persons and property subject to their control.

(1) Access control is a key component of the Installation's protection program. Installation access control standards shall include identity proofing; vetting; determination of fitness of an individual requesting and/or requiring access to Installations, and the issuance of local access credentials. Access control procedures and processes as part of the Installation's AT Plan shall have clearly documented tactics, techniques and procedures, which are essential in providing clear and consistent access control to the installations.

(2) Access control is defined as physical security (PS) measures that include PS equipment, personnel, and procedures used to protect installations and Navy assets from possible threats.

b. Installation access control plans will address the following:

(1) Types of Access

(a) Unescorted individuals.

(b) Escorted individuals.

31 MAR 2014

(2) Other considerations for controlling installation access include but are not limited to:

- (a) Escort qualifications, responsibilities, and authorizations.
- (b) Sponsorship qualifications, responsibilities, and authorizations.
- (c) Access privileges at each FPCON.
- (d) Mission-essential personnel program designation.
- (e) Emergency response designation, if applicable.
- (f) Day and time designation for access.
- (g) Locations authorized for access.

2. Procedures

a. Escorts. Escorts must remain with the visitor at all times while within the confines of the installation/facility. Escorts may be civilian or military personnel employed by, or attached to, the visited activity, and shall normally be from the office of the person being visited. A major objective in escorting visitors around a facility is to ensure that all material brought into the facility by the visitor is left with someone who can open and examine the contents, and that visitors leave no packages or other materials behind on their departure. Escort procedure may be used during FPCONs NORMAL, ALPHA, and BRAVO, and as addressed in the AT Plan.

NOTE: Contractors are not authorized to serve as escorts.

b. Trusted Traveler. Trusted Traveler procedure allows a uniformed service member or Government employee with a valid CAC ID, a military retiree (with a valid DoD ID credential), or a dependent (with a valid DoD ID credential), to present their ID token for verification while simultaneously vouching for any vehicle occupants. The number of personnel a Trusted Traveler is allowed to vouch for and/or sponsor at any one time can be specified by the Installation CO or designated representative. Members identified as Trusted Travelers are responsible for the actions of all occupants for whom they vouch and for meeting all escort security requirements as established in this instruction.

31 MAR 2014

Trusted Traveler procedures may be used during FPCONS NORMAL, ALPHA, and BRAVO. **Trusted Traveler procedures are prohibited in FPCON C and D unless authorized by the Regional Commander.**

NOTE: Contractors are not authorized to serve as trusted travelers.

c. Sponsor. Sponsor procedure allows a uniformed service member or Government employee with a valid CAC ID, a military retiree (with a valid DoD ID credential), or a dependent (with a valid DoD ID credential), to sponsor a visitor that requires installation access. The sponsor shall submit the required information to the Visitor Control Center (VCC)/Pass and ID Office: full name, SSN, start and end date, date of birth (DOB), installation to be visited, and facility to be visited. Once the visitor's background has been vetted, they can be issued a Visitor Pass/Badge. Pass and ID clerks will be responsible to verify the person receiving the special pass has the proper credentials listed in Table (1). Most installation visitors will fit into this category.

Escort procedure may be used during FPCONS NORMAL, ALPHA, and BRAVO and as addressed in the AT Plan.

NOTE: Contractors are not authorized to serve as sponsors.

d. Visitor Control Center (VCC)/Pass and ID:

(1) The VCC will ensure that all visitors have a completed NCIC, SORNA, Terrorist Screening database, and a local no-entry and barment list check.

(2) The VCC will determine denial of installation access. The establishment of standards for base access is ultimately the responsibility of the Installation CO. Any adverse information identified during criminal history checks will be evaluated by a competent authority. Likewise, positive mitigating factors should be considered in the final determination. The following minimum standards will be considered for denying installation access for a civilian employee, contractor, subcontractor, or family member:

(a) Any felony conviction within the past 10 years, including felony arrest not adjudicated or deferred.

(b) Any conviction of an offense meeting the sexual offender criteria.

31 MAR 2014

(c) Any misdemeanor conviction within the past 5 years, to include illegal possession and/or distribution of drugs, crimes of violence, sexual assault, larceny, and habitual offender. Additionally, a misdemeanor arrest not adjudicated or deferred.

(d) Any history of membership in any organization that advocates the overthrow of the U.S. Government.

(e) Barment from any DoD installation, which includes reciprocal barment from all installations.

(3) If anyone fails the background screening process, they will be added to a No Entry list. This list will be available to all CNRMA installations. The VCC personnel must consult this list before the issuance of local passes.

(4) Personnel who fail the background screening may submit a waiver. Waivers submitted for endorsement will be initiated by the Contractor's/Vendor's sponsoring CO (example: roofing contractor submits their waiver through NAVFAC) for consideration by the Installation CO with concurrence from the Regional Commander's representative. Approved waivers will only be honored for that specific installation. A denied waiver will be applicable to all installations.

(5) Waiver requests from EID Passport for NCACS failures will be processed through the Regional Security office. The Installation Commanding Officer will be notified of the approval/denial recommendation, the reason for the EID failure and the basis for the CNRMA recommendation. The Regional Security office will forward the decisions of the Commanding Officers to EID Passport once received.

e. General step-by-step procedures for visitors that require passes. Most installation visitors will fit into this category.

NOTE: Access requests will be submitted at least 5 days in advance.

(1) **Step 1:** The Sponsor or sponsoring agency will provide to the VCC the full name, SSN, start and end date, date of birth (DOB), installation to be visited, and facility to be visited.

(2) **Step 2:** The VCC submits request data to the Personnel Screening Center (PSC) for vetting. The PSC is

31 MAR 2014

physically located in the Regional Security Directorate, Norfolk, VA.

(3) **Step 3:** The PSC will conduct the required background checks and update the Visitor Access Control List (cleared/denied) on the CNRMA Share Drive.

NOTE: It is imperative Pass and ID Clerks verify latest background check is clear

(4) **Step 4 Vetting Results:**

(a) **Cleared:** The visitor can be issued a visitor pass/badge. Visitor passes should be issued for the duration of the visit, but not to exceed 30 days. Badges can be issued, not to exceed 1 year. Pass and ID clerks will be responsible to verify the person receiving the visitor pass has the proper credentials listed in Table 1.

(b) **Denied:** The visitor **WILL NOT** be issued a visitor pass/badge. Pass and ID clerks will give the visitor the following:

You have been denied access to Naval Station, XXXXXX.

The denial was based on an extensive background check. There are several reasons you could have been denied -

A criminal conviction, sexual offense, misdemeanors, affiliation with an organization that advocates the overthrow of the U.S. Government, you have been barred from another Navy Installation, or there is derogatory information within the Navy Law Enforcement Database.

Since the Criminal History was determined by name and date of birth check on NCIC, and cross verified with SSN, it's possible that a denial based on these factors could be mistaken. If you believe that the Denial Criteria does not apply to your criminal record, the applicant should request his **OWN** record by submitting a request and fingerprint cards to the FBI and pay \$18.00. The instructions on how to do so are at:

<http://www.fbi.gov/about-us/cjis/nics/general-information/cgbrochure.pdf>

If you believe this is in error, you can file a request for a waiver. The waiver should be initiated by the sponsoring command CO with supporting documentation to the installation CO with endorsement from the security department.

31 MAR 2014

(5) **Step 5:** All requests for waivers will be adjudicated. The Visitor Access Control list will be annotated. The sponsor/sponsoring agency will be contacted with adjudication results.

(6) **Step 6. Access:** Entry Control Point (ECP) personnel will compare the visitor pass/badge against a valid credential before every entry.

(7) Visual match of the photograph on the card to the person presenting the ID.

(8) Comparison and visual review of the card for unique topology and security design requirements. The visual check of the card will include verifying authenticity by checking the anti-counterfeit and/or fraud protection measures embedded in the credential.

NOTE: Off Hours/After hours: Delivery personnel, TWIC card holders, vendors, visitors and any personnel not in possession of a valid access credential (CAC, TESLIN, NCAC, or installation pass) will not be granted access until vetted at the Entry Control Point. Vetting will be accomplished by notifying the dispatch center that an unvetted visitor is present for entry and providing the contact information for the sponsor, as well as the full name and date of birth of the visitor. The dispatcher will contact the sponsor to verify need for access. After the sponsor has verified need for entry, the dispatcher will run a NCIC Criminal history check, check the Department of Justice SORNA site for Sex Offender status, and check the CLEOC Debarment database to see if the individual has been barred from any Navy Installations. If the visitor meets any of the denial criteria the sentry will be notified that access is denied. If access is granted, the sentry will issue a one day VISITOR pass and grant access.

If vetting is not possible (systems are down) Escort/trusted traveler procedures shall be employed or entry will be denied.

f. Identification Authorization, Authentication, Credentialing, and Access. A combination of active and passive measures will control access to an installation. The processes of identification authorization, authentication, credentialing, and granting access must be uniform and integrated. Personnel access identification-checks will continue to be performed until upgraded or replaced with Federal Personal Identity Verification (PIV) compliant systems (e.g., NCACS).

31 MAR 2014

(1) Only personnel delegated by the Installation CO shall perform access control duties that include:

- (a) Identity-proofing.
- (b) Vetting and determination of fitness.
- (c) Access authorizations and privileges.

31 MAR 2014

List of Personal Status, Access Credential, and Required Vetting

*All need to meet Identity-proofed requirements of Table (1).

<u>Status</u>	<u>Access Credential</u>	<u>Vetting</u>
Active Duty Military	CAC	Not required
Reserve	CAC	Not required
Foreign Military TDY	CAC	Not Required
DoN Civil Service	CAC	Not Required
Dependents	Military ID	Not required
Military Retirees	Military ID	Not required
Foreign Military Dependents	Military ID	Not Required
Law Enforcement	LE Credential	Not required
Other U.S. Government	USG-issued Federal PIV Credentials	Not Required

Note: Includes OPM investigators with US Access credential gold badges (GS) or silver badges contract OPM investigators IAW Access Control Advisory 10082012.

Unescorted Family Members		
Non-Dependant	Visitor Pass	Required
Unescorted visitor	NCACS/Day Pass	Required
Contractors	NCACS/Day Pass	Required
Vendor	NCACS/Day Pass	Required
PPV Housing	Badge	Required
Volunteers	Badge	Required
Dependent's Agent	Badge	Required
Merchant Seaman	Visitor Pass	Required
Student	Badge	Required
MWR	Visitor Pass	Required
Navy Guest	Visitor Pass	Required
Randolph Sheppard		
Act blind vendors	Badge	Required
Transportation Worker	TWIC with bill of lading or confirmed pick-up	Required
Taxi drivers	Badge	Required

31 MAR 2014

Note: Taxi drivers participate in the Single Source Coordinator program sponsored by the NEX and pay a service fee for processing, inspection of vehicles, and confirmation of liability insurance requirements. As such, they do not participate in NCACS, but are sponsored by the NEX, screened by the PSC and issued an installation or regional badge for credentialing.

Note: Law Enforcement

State Police officers in a marked or official unmarked vehicle will be allowed to enter and/or depart unescorted and without a pass through any installation gate when conducting business at one of the regional installations.

Local municipal police officers in marked and/or official unmarked vehicles will be allowed entry through any gate unescorted and without a pass through any installation gate when conducting business at one of the regional installations.

- In order to prevent regional installations from becoming a haven for persons fleeing the authority of the civilian police, local law enforcement agencies shall be passed into the installation unimpeded, when in "hot pursuit" of fleeing suspects.
- The sentry will immediately notify the Emergency Communications Center/Dispatch whenever a civilian police vehicle is allowed to enter under "hot pursuit" circumstances.
- Members of the installation's Security Precinct will proceed to the scene of activity/incident upon receiving information that a civilian police vehicle has entered the installation in "hot pursuit."

31 MAR 2014

Table 1

List of Acceptable Documents - All Documents Must Be Unexpired.*(One from List A or one from each of Lists B and C.)*

<u>List A</u> Documents that Establish Both Identity & Employment Eligibility	O R	<u>List B</u> Documents that Establish Identity	A N D	<u>List C</u> Documents that Establish Employment Eligibility
<ul style="list-style-type: none"> • U.S. Passport • Certificate of U.S. Citizenship (Form N-560 or N-561) • Certificate of Naturalization (Form N-550 or N-570) • Foreign Passport w/I551 stamp or attached Form I-94 indicating unexpired employment authorization. • Permanent Resident Card or Alien Registration Receipt Card with Photo (Form I-151 or I-551) • Temporary Resident Card (Form I-688) • Employment Authorization Card (Form I-688A) • Re-entry Permit (Form I-327) • Refugee Travel Document (Form I-571) • Employment Authorization Document issued by Department of Homeland Security (DHS) that contains a photo (Form I-688B) 		<ul style="list-style-type: none"> • Driver's License issued by a state or outlying possession of the U.S. that contains photograph or info such as name, DOB, gender, height, eye color, and address. • ID Card issued by Federal, state, or local Government agency that contains a photo, or info such as name, DOB, gender, height, eye color, and address. • School ID Card with Photo • Voter Registration Card • U.S. Military Card or Draft Record • Military Dependent ID Card • U.S. Coast Guard Merchant Mariner Card • Native American Tribal Document • Driver's license issued by a Canadian Government authority 		<ul style="list-style-type: none"> • U.S. Social Security Card (other than a card stating it is not valid for employment) • Certification of Birth Abroad issued by the State Department (Form FS-545 or Form DS-1350) • Original or Certified Copy of a Birth Certificate issued by a state, county municipal authority, or outlying possession of the U.S. bearing an official seal. • Native American Tribal Document • U.S. Citizen ID Card (Form I-197) • ID Card for use of Resident Citizen in the United States (Form I-179) • Employment Authorization Document issued by DHS (other than those listed in List A).

31 MAR 2014

VISITOR CONTROL CENTERS

Regional Installation Pass Office hours and days of operation vary; call one of the offices listed below for details:

Navy Region Mid-Atlantic, Norfolk, VA

M-F 0700-1500 Regional Visitor Control Center (RVCC)
 (757) 322-2753
 DSN: 262-2753

Naval Station Norfolk, VA

M-F 0600-1600 (757) 322-2968

Naval Station Newport, RI

M-F 0700-1530 (401) 841-3126/(401) 841-3388
 Naval Undersea Warfare Center Division (NAVUNSEAWARCENDIV)
 M-F 0630-1530 (401) 832-2152/(401) 832-2153

Joint Expeditionary Base Little Creek-Fort Story, Virginia Beach, VA

Little Creek
 M-F 0700-1500 (757) 462-3999/4001
 Fort Story
 0730-1630 (closed 1300-1400) (757) 422-7195

Naval Weapons Station Yorktown, VA

M-F 0645-1645 (757) 887-7338/7339

Naval Weapons Station Earle, Colts Neck, NJ

M-F 0630-1600 (732) 866-2243/(732) 866-2214

Naval Air Station Oceana, Virginia Beach, VA

M-T 0600-1700 (757) 433-2816/(757) 433-3212
 F 0600-1600
 Sun 1300-1500

Norfolk Naval Shipyard, Portsmouth, VA

M-F 0600-1630 (757) 396-5076/7260/3090

Portsmouth Naval Shipyard, Portsmouth, NH

M-T 0630-1500 (207) 438-2235/2614/2135
 F 0630-1430 DSN: 684-2235/2614/2135

Naval Submarine Base New London, Groton, CT

M-T 0600-1800, F 0600-1400 (860) 694-4030

31 MAR 2014

VISITOR CONTROL CENTERS

Surface Combat Systems Center Wallops Island, VA

M-F 0700-1600 (757) 824-2058

Naval Computer and Telecommunications Area Master Station
Atlantic, Detachment Cutler, ME

M-F 0700-1500 (207) 259-8267

Naval Support Activity Saratoga Springs, NY

M-F 0800 - 1530 (518) 886-0200 x 110

Naval Support Activity Philadelphia, PA

M-F 0630 - 1500 (215) 697-2609

Naval Support Activity Hampton Roads, Northwest Annex,
Chesapeake, VA

M-F 0700-1500 (757) 421-8123

Naval Support Activity Mechanicsburg, PA

M-F 0600-1600 (717) 605-2276/1750/5176

31 MAR 2014**Access Control for Senior Officer Functions**

1. Purpose. To grant Navy Region Mid-Atlantic (NRMA) installations with relief from the access control requirements of reference (a) and provide specific direction for support of senior officer events occurring on-installation.
2. Intent. Provide clear guidance to installations, guests, and support staffs on reduced access control procedures for distinguished visitors and minimize potential embarrassment of invited guest(s) and associated host(s).
3. Background. CNRMA Access Control Program compiles higher headquarters requirements and NRMA specific execution of routine escorted/unescorted installation access control. The spirit and intent of existing guidance is to protect the installation from unaffiliated personnel whose character cannot be confidently vouched for and may thereby present an unacceptable risk to the safety and security of the installation. Reference (a) and associated source requirements do not accommodate prudent relaxation of screening requirements for unaffiliated persons who, by the nature of their position or community standing, may reasonably be presumed to meet screening requirements.
4. Applicability. This directive is applicable to all senior officer (O-5 and above) events conducted on-installation when unaffiliated civilians are invited guests at any installation or activity.
5. Responsibilities
 - a. Host Officer
 - (1) Provide event notification to the Installation CO. This notification should be provided with adequate time (when invitations are sent) for the Installation CO to ensure information dissemination to all coordinating parties.
 - (2) Designate a representative to coordinate with the Installation Public Affairs Officer (PAO)/Protocol Officer.
 - (3) Provide a list of invited guests to the Installation CO at least 24 hours prior to the scheduled date and time of the event.
 - (4) Ensure all guests are provided with instructions and directions as coordinated with the installation.

31 MAR 2014

(5) Notify guests that official picture identification will be required for installation access (e.g. driver's license, passport).

(6) Coordinate with installation and provide necessary signage to event parking as necessary.

b. Installation Commanding Officer. Installation COs will ensure coordinated execution of this process to promote the highest degree of diplomatic protocol and expedite invited guests to senior officer functions at on-installation locations. Specific items for consideration and coordination:

(1) Provide access list and/or invitation sample to appropriate entry control points.

(2) Brief gate sentries on the event, access authorization, location of event, and driving directions from their post to the designated guest parking.

(3) Grant guest access upon presentation of picture identification and validation against the host officer's guest list.

(4) Coordinate host officer's signage at installations where written or oral driving directions will be overly complicated.

(5) Support reservation of designated parking for guests.

6. Execution. This policy is directive in nature and will be executed at the installation level. No waivers or additional plans are required for CNRMA approval.

31 MAR 2014

Special Event Antiterrorism Plan (SEAT) Guidance

1. Purpose. To provide specific guidance to all COs and or officers in charge (OIC) in the CNRMA AOR on the development of Special Event Antiterrorism plans (SEAT) for approval by CNRMA. To aid in meeting this purpose, the CNRMA Anti-Terrorism Officer (ATO) seeks to:

- a. Provide conceptual understanding of the SEAT.
- b. Standardize SEAT submissions by use of a template.
- c. Define routing procedures and timelines.
- d. Define when SEATs should be submitted.

2. Background. Reference (c) requires the application of specific risk analysis and development of AT plans for special events involving gatherings of more than 300 personnel. This is particularly important when combining the special event with a location outside the protective perimeter of an installation or military controlled facility. Reference (l) and (n) amplify the requirements outlined in reference (c) and provide specific limitations on the use of Navy Security Forces (NSF) off installation to minimize the commander and individual risk to an inadvertent violation of the Posse Comitatus Act. To date there has been limited guidance provided for specific details on the content and format of a SEAT. This document provides clarity on the development of SEATs and outlines the approval process.

3. Applicability. AT considerations must be factored into all event planning. This policy applies to all Navy Installations, tenant commands of Navy installations, and off-installation activities subject to the Navy Component Commander in the CNRMA AOR for the execution of a special event on, or off installation.

4. Requirement triggers. Most events occurring within an installation perimeter should be covered by the installation's AT Plan and routinely re-occurring events may be covered by a standing Event AT Plan. Events operating outside the parameters of these existing plans will require the development of a SEAT, utilizing enclosure (4) for assistance in determining when an SEAT should be developed. The following instances (not all inclusive) are examples of when a SEAT should be submitted and the level of approval that should occur.

31 MAR 2014a. On-Installation Events

(1) Public Visitation/Access. Any instance of general public visitation (GPV) to a Navy Installation within the CNRMA AOR will require a SEAT approved by the Region Commander per reference (1). Further definition of the distinction between GPV and controlled group tours is provided in paragraphs (a) and (b) below. If the event is considered a pre-arranged controlled group tour the plan may be approved by the Installation CO; all others must be approved by CNRMA. Events occurring on U.S. Navy property outside the installation perimeter are considered off-installation events.

(a) GPV is defined as an instance where the base or a portion thereof, is open for general public access without prior screening or escort. An example of such an event is the Naval Air Station Oceana Air Show. The gate is opened and people are allowed access to the installation without regard to their affiliation.

(b) Pre-arranged controlled group tours are sponsored events where DoD affiliated personnel provide an escorted tour to a group of unaffiliated people. These events generally are for the purpose of increasing awareness of the Navy and its mission but could simply be for the purpose of a school field trip. Tours may be arranged for various organizations that include: students from high schools or colleges, Boy/Girl Scouts, Youth Clubs, Chamber of Commerce, City Council members, foreign dignitaries, celebrities, etc. Invitation only events where guests are provided advance guest passes and are hosted at a designated location(s) are treated the same as pre-arranged controlled group tours in this guidance.

(c) Military Welfare and Recreation (MWR) events may be categorized as GPV or Pre-arranged controlled group tours, when an event is open to unaffiliated personnel, depending on the level of participant control exercised. If there are no controls applied to an event and it is open to the general public then it will be considered GPV. An event may only be considered a pre-arranged control group tour if participants are only allowed escorted access.

(2) Instances where non-organic armed security forces will be on the installation requires an Event AT Plan to outline the integration of armed personnel into the overall C2 construct and must be approved by the installation CO.

31 MAR 2014

This may be visitation by foreign dignitaries or U.S. high risk personnel (POTUS, VPOTUS, CNO, etc.) accompanied by protective details and or law enforcement roles and responsibilities. A good rule of thumb is that if the event requires a 5050 then special AT consideration should be given and measures taken to ensure security requirements are adequate for the event.

(3) Events not otherwise covered by the installation AT Plan or standing event specific AT plans will require a SEAT. Approval level for other plans will be situation dependent and will be coordinated with the CNRMA ATO.

b. Off-Installation Events. These events present a unique challenge due to stringent limitations on the use of NSF off-installation. Events where increased security is required, it is imperative that the planning staff coordinate with local law enforcement, licensed private security, or venue security personnel to ensure adequate measures are in place to provide a safe and secure environment.

(1) Events occurring off-installation where the number of DOD personnel (military, civilian, or dependents) are expected to exceed 300 personnel will require a SEAT approved by the Region Commander.

(2) All events where less than 300 DoD personnel will be in attendance will still require specific security consideration and should be addressed in the event plan; however, for events between 150 and 300 personnel a SEAT is required for approval by the installation/activity/unit CO/OIC.

(3) Events where local law enforcement capabilities do not sufficiently mitigate the threats identified in the risk assessment process or where local law enforcement is requesting the assistance of NSF to meet shortfalls, commanders must fully evaluate, meet, and request to employ NSF off-installation per the requirements of reference (n).

5. Concept. Special events and general public visitation on and off installation present unique situations where advance security coordination with the CNRMA Regional Security Officer, local law enforcement (LLE), site security coordinators, and contract security is essential. The SEAT is a tool that serves to build a picture of the security posture for CNRMA's approval.

31 MAR 2014

It should outline the level of coordination or measures taken to provide security for a special event with due regard to the current real-world threat. The SEAT plan will be submitted/approved (depending on approval level requirements) by the CO/OIC of the command initiating the SEAT or a person designated to have by direction authority to assume risk on behalf of the CO/OIC. At a minimum, the SEAT will contain:

a. AT Risk Management. As with any AT Plan, a risk assessment is critical for the identification of what the threat is, what the critical assets are, and what vulnerabilities need to be mitigated. The result of this assessment should be the basis for the development of the SEAT.

(1) When populated, the risk assessment tools are classified, at a minimum, confidential and should be transmitted to the approving official via SIPRnet.

(2) The CNRMA ATO will provide an Excel spreadsheet, to those that desire it, to aid in the risk assessment process. This spread sheet provides a standardized layout for the threat assessment, criticality assessment, and vulnerability assessment with pre-defined and weighted values.

b. AT working group (ATWG). The SEAT should be accomplished with the assistance of the command's ATWG to ensure all command stakeholders have visibility of the plan and input to the process.

c. Basic Format Elements. These elements are required as the minimum baseline for plan submissions. If a circumstance exists that renders one of these items irrelevant then the item will remain as a place holder but be annotated as "Not Applicable." The basic format is outlined in enclosures (5) through (7), which contained the following elements:

(1) Situation. Provide a general summary of the entire event to be held. If off installation, state if the attendees will be in uniform and the presence of known high risk personnel.

(a) Friendly Forces. List all forces involved in the security plan.

(b) Enemy Forces. Reference the threat assessment.

31 MAR 2014

(c) Threat Summary. The threat summary should be kept at the unclassified level and provide a general understanding of the most probable avenue of attack.

(d) Assumptions. List all assumptions that were figured into the development of the AT Plan. Examples of common assumptions are (not all inclusive):

1. The current FPCON will not change between the date of the plan and the date of the event.

2. The event, or its location, has not been the subject of criminal or terrorist surveillance and/or planning.

3. The measures provided herein will project the image of a hard target to potential adversaries.

(e) Mitigation Ability. Provide an overt statement indicating that the security provisions outlined in the SEAT mitigates all assessed threats within an acceptable threshold and that the CO is comfortable assuming any remaining risk associated with the event.

(2) Mission. Provide a basic mission statement that supports development of a safe environment for the execution of the event. It should contain inclusion of any supporting elements that will be involved with the security plan.

(3) Execution. Provide an overall concept of operations. This should draw a mental picture of the "who, what, when, where, and how" of the security construct. To meet that end, the execution portion of the plan should contain:

(a) Commander's Intent. This is generally an echo of the mission statement but may contain additional specific information that details how the security will be organized.

(b) Task Organization. Every organization that plays a part in the execution of the event should be listed here with their particular responsibility.

1. NSF: (On installation only) Outline all specific tasking (i.e. access control, traffic control, security patrols, baggage screening, emergency response, etc.).

31 MAR 2014

2. Civilian Law Enforcement: Outline all specific tasking (i.e. access control, traffic control, security patrols, baggage screening, emergency response, etc.).

3. Contract Security: Identify the contractor and outline all specific tasking (i.e. access control, traffic control, security patrols, baggage screening, emergency response, etc).

4. Fire and Emergency Services: Outline all specific tasking (i.e. establishment of first aid tent, onsite presence, etc.).

5. Other Agencies: Many events will be sponsored by or supported by outside agencies and they should be involved / included in the AT planning. There are a multitude of entities reaching out to support the morale and welfare of our military and some of these organizations include: The Navy League, MWR/ITT, The Red Cross, USO, etc. The SEAT needs to outline what part they play in the plan (i.e. providing an access list of invited guests, reception and screening of guests, logistic support etc.).

6. Minimum required elements must cover:

- a. Training
- b. Additional security posts
- c. PPRs
- d. Access control procedures
- e. Crowd control/mass evacuation
- f. Personnel screening for the general
- g. Baggage restrictions and screening
- h. Screening and securing of tour buses

public

31 MAR 2014

i. Signs notifying the public of rules and regulation.

(c) Use of Force. If NSF is employed, a positive statement indicating that the standing rules for the use of force (SRUF) are in effect is required. If there are any authorized deviations from the SRUF it will be indicated in this section. When the event will be held off installation and local law enforcement are unable to support, the sponsoring agency may hire armed contract security and the commander will coordinate with the contractor and Staff Judge Advocate to develop and provide rules for the use of force for the event. If civil law enforcement authorities are solely responsible for the security of the event then indicate so.

(4) Administration and Logistics. Provide any event specific information and identify parties that support the procurement process.

(a) Training. List any event specific security training that has been or will be held. Specific examples include identification of event-specific access passes, pre-planned responses, SRUF, traffic control routes, lost child procedures, etc.

(b) Event Briefs. Outline the briefs to be held and the presenting entity.

(c) Logistic Support. Identify the responsible parties for event logistics support (i.e. presentation equipment, barriers, signs, etc.).

(5) Command, Control, and Communications. Define the operational relationship between the supporting and supported elements. Identify the method of communications (primary, secondary, and tertiary) and reporting channels.

d. Other SEAT Elements. Enclosures to the SEAT should include, but not be limited to:

(1) Event layout diagrams - to include graphic representations of force disposition, traffic routes, parking areas, and evacuation routes.

(2) Watch bills.

(3) Risk assessment products.

31 MAR 2014

(4) Examples of special passes designed for the event.

(5) Points of contact.

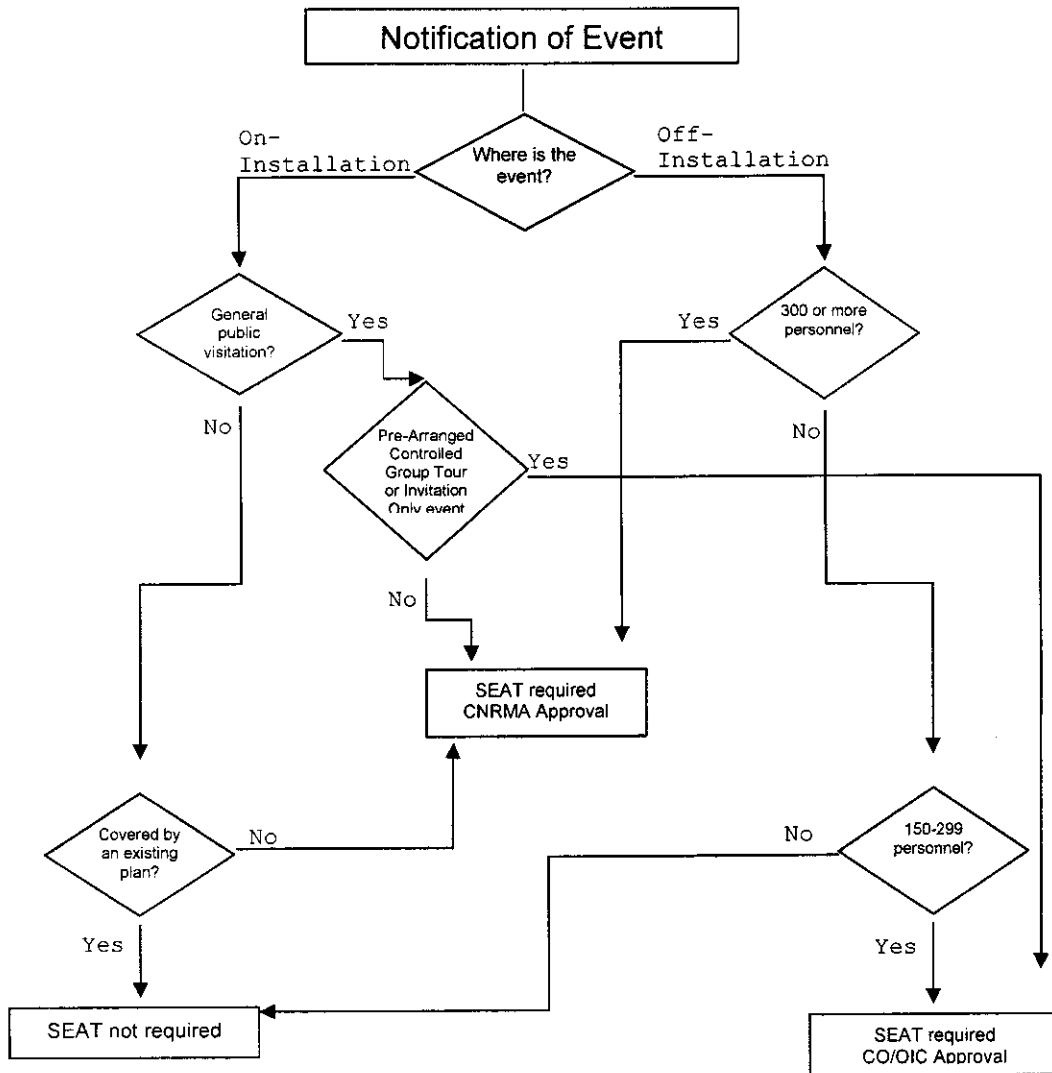
6. SEAT Routing Chain. Tactical control for force protection (TACON for FP) in the NORTHCOM AOR for Navy elements flows from NORTHCOM to the Navy Component Commander (USFFC) to the Regional Commander (CNRMA) to the Installation Commander and finally to installation tenant commands. Units/organizations not residing within the protective perimeter of an installation fall directly under the Regional Commander (CNRMA). Routing of all SEATs will follow the TACON for FP to CNRMA for approval.

7. Timeline. SEATs will be submitted to the CNRMA ATO no later than 30 days prior to the event. Best practice dictates that command ATOs coordinate with the CNRMA ATO for review and feedback prior to plan submission to minimize rework and expedite the approval process.

8. This guidance is effective immediately and will remain effective until superseded or canceled. Direct all questions or concerns to the CNRMA AT shop: (757)445-0786, (757)322-2911, (757)322-2956.

31 MAR 2014

FOR OFFICIAL USE ONLY

Seat Decision Flow Chart

General Public Visitation (GPV) is defined as an instance where the base or a portion thereof is open for general public access without prior screening or escort. An example of such an event is the Oceana Air Show. The gate is opened and people are allowed access to the installation without regard to their affiliation.

Pre-arranged controlled group tours are sponsored events where DoD affiliated personnel provide an escorted tour to a group of unaffiliated people. These events generally are for the purpose of increasing awareness of the Navy and its mission but could simply be for the purpose of a school field trip. Tours may be arranged for various organizations that include: students from high schools or colleges, Boy/Girl Scouts, Youth Clubs, Chamber of Commerce, City Council members, foreign dignitaries, celebrities, etc.

31 MAR 2014**Sample SEAT submission template - On-Base (Large)**

CLASSIFICATION - (per enclosures)

From: Commanding Officer, Naval Station Springfield
To: Commander, Navy Region Mid-Atlantic

Subj: SPECIAL EVENT ANTITERRORISM PLAN - METALLICA CONCERT

Ref: (a) (S) NCIS Threat Assessment (Date)
(b) (S) Event Specific Risk Assessment
(c) NAVSTA SPRINGFIELD OPOD AT-3300
(d) DoD DTM 09-012
(e) DoDI 2000.16
(f) COMUSFLTFORCOM OPOD 3300 (Series)
(g) USFF Force Protection (FP) Directive 11-009
(111900Z MAY 11)
(h) COMNAVREGMIDLANT OPOD-AT 3300.1

Encl: (1) Event Layout
(2) Watchbill - Additional Watches
(3) Event Specific PPRs
(4) CO's Guest Pass

1. Situation. In accordance with references (a) through (h), the following information is provided. On Saturday, 31 December 2011 from 2100 to 0030 1 January 2012 Naval Station Springfield (NSS) will host a Metallica concert at the NSS sports complex track and field to celebrate and bring in the New Year. NSS expects participation to exceed 1000 military, DOD civilian, and dependents. This is not a general public visitation event; however, Commanding Officer (CO) NSS will have unaffiliated civilian guests. This event has only been advertised within the installation communication channels (base newspaper, posters, and MWR representatives). Information on the event is publically available via the installation and MWR web sites; however, the NSS Public Affairs Officer has not received information requests from the general public and the local media has not yet reported on this event.

a. Friendly Forces

- (1) NSS Navy Security Force (NSF).
- (2) Springfield Police Department (SPD).
- (3) Navy Criminal Investigative Service (NCIS).

Enclosure (5)

31 MAR 2014

(4) NSS Fire and Emergency Services (FIRE).

(5) Intercity Life Flight (ILF).

(6) NSS Explosive Ordnance Disposal Detachment (EOD).

b. Enemy Forces. See reference (a).

c. Threat Summary. NSS has conducted a risk assessment, reference (b), based on the information contained in reference (a). With due consideration to the current FPCON and the standing security measures for NSS, a backpack IED or an active shooter scenario are the most likely threats to this event.

d. Assumptions. The following assumptions were used in the development of this plan:

(1) The current FPCON will not change before execution of the event.

(2) NSS is not actively being targeted.

(3) The measures provided herein will project the image of a hard target to potential adversaries.

e. Mitigation Ability. NSS surveillance detection team has not identified any hostile surveillance activity that would indicate criminal or terrorist surveillance and/or planning nor does reference (a) indicate any specific threats. NSS CO is confident that the security provisions outlined herein effectively mitigate potential risks to NSS assets and personnel and is comfortable that this event does not present any appreciable risk.

2. Mission. Conduct force protection operations in support of the New Year Celebration Concert. Mission objectives are as follow:

a. Provide a safe and secure environment.

b. Deter and detect terrorist and criminal threats.

c. Should an event occur, mitigate the effects of a terrorist or criminal act.

d. Should an event occur, recover from a terrorist or criminal act.

31 MAR 2014

3. Execution

a. Commander's Intent. Execute a robust security environment to protect the installation, assets, service members, civilian support staff, and guests attending the New Year Celebration concert.

b. Concept of Operations. This plan outlines three phases of operations.

(1) Phase 1 - The planning and coordination outlined herein constitute this phase.

(2) Phase 2 - Execution of the event and this plan.

(3) Phase 3 - Return the installation to normal baseline force protection posture and capture any lessons learned.

c. Task Organization. The following outlines the participating organizations and their assigned roles:

(1) NSS NSF:

(a) Coordinate a threat mitigation/reduction strategy with all supporting elements. Strategy includes a layered security plan from the NSS perimeter to the event location. NSF will establish a Security Tent within the perimeter of the venue to serve as a local command and service center during the event. The layered defense will include:

1. Friendly Forces: See enclosure (1) for disposition of forces.

2. Access control: Conduct routine access control in accordance with standing Standard Operating Procedures (SOP). Additionally, the following security measures will be taken:

Note: If conducting General Public Visitation, describe how access will be controlled/managed with a particular emphasis on describing the confines of the installation within which the visitation will take place.

a. Buses. Due to limited parking on the installation and in order to support appropriate standoff distances, NSS has established an off-site parking area at the NEX/Commissary complex.

31 MAR 2014

Two buses will transport members between the parking area and the event location. Buses will be swept for explosives by MWD at 1800 in preparation for the first bus run at 1900. The buses will remain under positive control with 1 NSF onboard. The NSF member will verify the identification of all personnel boarding the bus for credentials meeting the NSS access control SOP. Personnel in possession of CO's Guest Passes will be directed to Gate 1 for directions to the designated parking area.

b. POVs/Rental Vehicles. Personally-owned vehicles (POVs) and rental vehicles must meet the NSS access control SOP guidelines unless the driver is in possession of a CO's Guest Pass. CO's guests will be validated against the guest list and all parties entering the base will be required to show valid picture identification. Once validated, CO's guests will be provided a standard dashboard vehicle pass and directions to the guest parking area.

c. CO's Guest Passes. Passes will be issued by the NSS PAO. See enclosure (4) for an example pass.

d. Baggage. Base advertisement for this event has included messaging indicating that large bags and coolers will not be permitted at the event. All hand baggage will be subject to visual inspection by NSF personnel at the event ECP.

3. Parking. NSS has established a standoff distance of 300 ft from the event location to support the large gathering and to mitigate any potential VBIED concern. The designated parking areas are in the "South Lot" near the Supply Center and the "West Lot" near the Public Works Warehouse. Random patrols of the parking areas will be conducted by NSS NSF.

4. Traffic Control. NSS ASF will provide parking assistance to support smooth movement of traffic into the parking areas. One ASF member will be stationed at the four-way stop intersection of Ticonderoga and Burke to expedite the flow of incoming traffic.

5. Quick Reaction Force (QRF). NSF will establish and maintain a QRF in the Security Tent for the duration of the event.

31 MAR 2014

6. Lost Child. NSF will handle lost children per the pre-planned response (PPR) developed for this event and included in the PPR section of this plan.

7. Crowd Control. A combination of armed sentries and unarmed personnel will be assigned to assist in crowd management.

8. Additional Watches. Enclosure (2) provides the additional watches NSF will stand up in support of this event.

(b) Use of Force. Rules for Use of Force (RUF). NSF RUF will be in accordance with CJCS 3121.01b and SECNAVINST 5500.29C. All personnel will be trained with regard to RUF.

(2) Springfield Police Department. SPD has confirmed their commitment to the NSS and SPD MOA. SPD will place a dedicated patrol vehicle and one officer outside Gate 1 at the intersection of Simpson Street and Ash Avenue from 1800 to 2200 on 31 December and from 0000 to 0200 on 1 January.

(3) Fire and Emergency Services. FIRE will provide onsite EMS service with two personnel and an EMS Vehicle stationed inside the event perimeter at the First Aid tent.

(4) MWR. Will provide NSF with a complete list of the concert support crew and staff. Additionally, MWR will coordinate with event staff to ensure that all support vehicles are processed at the commercial vehicle inspection area per standing SOP.

(5) Public Works. In coordination with the PAO, Public Works will ensure signage is posted for the traffic route to guest parking.

(6) Public Affairs. The Public Affairs Officer is the principal point of contact for all of the CO's guests and will provide guests with invitations to the event. Additionally, the PAO will submit a list of invited guests to the Security Officer for validation at the entry control point.

4. Administration and Logistics

a. Pre-Planned Responses. In the event of an act of terror or threat to the installation, all responses will be in

3 1 MAR 2014

accordance with reference (c) and the special procedures list in this special event AT Plan. Reference (c) will be available at the Security Tent.

(1) Lost Child Procedures

(a) Proceed immediately with the person to the security tent located near the concert ECP.

(b) At the security tent, basic information will be gathered from the individual.

(c) Name, age, clothing, special instructions, medical issues.

1. If lost child is with security member and is wearing special Lost Child Wrist Bands given out at the ECP, then all information about the parent/guardian will be on the wrist band, and a cell phone number to call.

2. Call Cell phone number to locate parents.

(d) Lost child description will be relayed to dispatch and further passed on the security channel:

1. Security personnel in the parking areas and at the ECP's will pay close attention to personnel leaving the area for any children matching the description of the missing person.

2. ECP personnel will stop any vehicle/pedestrian with children, and verify that they do not match the description of the missing person, prior to allowing them to exit the base.

(e) Person initially contacted by parent/child shall remain with that person in the security tent until resolution.

(f) Upon resolution, security tent personnel will communicate this to dispatch to secure from the search.

(2) Flush Plan/Evacuation Procedures. All gates (with exception of Gate 3) will become outbound only gates during an emergency.

31 MAR 2014

(a) All security personnel will assist with expediting personnel to their vehicles in a safe and orderly fashion.

(b) Intersection traffic control will be re-manned to support expeditious outbound traffic flow.

(c) Pedestrians requiring return transport to the centralized parking area will be directed to gather on the south side of the track to await busing back to their parking area.

(3) Mass Casualty Event

(a) First Responders - Secure Scene. This will be accomplished before the care of personnel injured during the event.

(b) Additional Units will set perimeter.

(c) Fire Chief will assume duties as On Scene Commander for the event.

(d) Expand perimeter to ensure the scene is safe for any responding units.

(e) Establish entry point for Emergency services to access injured personnel, ensure all personnel who enter the scene are logged in and out of the scene.

(f) Ambulances and Emergency vehicles will enter and exit the base via Gate 3.

(g) Establish Press area at the Base Theater, where PAO can keep media informed.

(h) Direct personnel that have lost their guests or are lost from their guests to the Enterprise MWR Club as a meeting point.

(i) If event causes the concert to end, implement Flush/Evacuation Plan. Have personnel proceed to vehicles and follow Security personnel's directions for exiting the base in an orderly fashion.

1. If Emergency vehicles are using Gate 3; vehicles that are being flushed through Gate 3 will be halted to allow access for emergency vehicles to enter the base.

31 MAR 2014

(4) Crowd Control Pre-Planned response

(a) First responders - set a perimeter and wait for back up forces to arrive.

(b) Deploy Quick Reaction Force to the scene.

(c) If this is peaceful, control the flow of personnel guiding them towards their vehicles to exit the base. If this becomes a Protest follow the Protest PPR.

(d) Establish Press area away from the scene where PAO can keep media informed.

(e) If event causes the concert to end, implement Flush/Evacuation Plan. Have personnel proceed to vehicles and follow Security personnel's directions for exiting the base in an orderly fashion.

(5) In any situation not covered by Pre-Planned responses.

(a) First Responders - Secure Scene.

(b) Back Up units - Set perimeter.

(c) Expand perimeter to ensure the scene is safe for any responding units.

(d) Establish Press area away from the scene where PAO can keep media informed.

(e) If event causes the concert to end, implement Flush/Evacuation Plan. Have personnel proceed to vehicles and follow Security personnel's directions for exiting the base in an orderly fashion.

b. Training

(1) Base Wide Anti-terrorism Drills have been conducted to include:

(a) Mass Casualty

(b) Active Shooter

(c) ECP Penetration

31 MAR 2014

- (d) VBIED/PCIED
- (e) Surveillance
- (f) Suspicious Package

(2) Special training will be conducted 12 December 2011 and 15 December 2011 for:

- (a) Review of concert AT Plan
- (b) Pre Planned Responses for all watch standers
- (c) Crowd control procedures
- (d) Lost Child
- (e) Medical Emergency
- (f) Flush Plan
- (g) Use of Force
- (h) Mass Casualty

(3) Guard mount conducted daily during December will emphasize following:

- (a) Lost Child procedures
- (b) Flush Plan
- (c) Use of Force
- (d) Medical Emergency
- (e) Mass Casualty
- (f) NSS concert AT Plan

c. Logistic Support. MWR is the sponsoring organization for this event. All requests for event logistics support will be submitted to NSS MWR Representative, Mr. Jack B. Fun (888-555-1234).

31 MAR 2014

5. Command, Control, and Communications. Security forces assigned to provide law enforcement/security and antiterrorism operations on Naval Station Springfield are under the operational control of the Installation CO. NSS Installation Security Director (ISD) is the direct representative of the Installation CO and will coordinate with all supporting agencies for execution of this plan. Navy Security Force personnel will not be employed off-installation (armed or unarmed). MWD and EOD are exceptions to use of military forces off-installation.

a. Command and control will be executed from security dispatch located at the NSS Security headquarters building. The command center will be manned by the NSS Security Force Watch Officer and dispatcher. The command center will maintain communications with all ECPs, area supervisors, QRF, event security tent, and other listed task organizations. All communications between military and local agencies will be handled through dispatch.

b. Communications

- (1) NSF Primary: TAC-1
- (2) NSF Alternate: TAC-2
- (3) VBPD: VBPD Dispatcher
- (4) NSS Fire: Dispatch
- (5) NSS Fire Alternate: Admin
- (6) NCIS: TAC-1, Cell Phone
- (7) EOD: TAC-1, Cell Phone

Commanding Officer Signature

31 MAR 2014Sample SEAT submission template - Off-Base

CLASSIFICATION - (per enclosures)

From: Commanding Officer, Navy Tenant Command
To: Commander, Navy Region Mid-Atlantic
Via: Commanding Officer, Host Installation

Subj: SPECIAL EVENT ANTITERRORISM PLAN - HOLIDAY PARTY

Ref: (a) (S) NCIS Threat Assessment (Date)
(b) (S) Event Specific Risk Assessment
(c) NAVSTA SPRINGFIELD OPOD AT-3300
(d) DoDI 2000.16
(e) COMUSFLTFORCOM OPOD 3300 (Series)
(f) USFF Force Protection (FP) Directive 11-009
(111900Z MAY 11)
(g) COMNAVREGMIDLANT OPOD-AT 3300.1

Encl: (1) Event Layout
(2) Watchbill - Additional Watches
(3) Event Specific PPRs
(4) CO's Guest Pass

1. Situation. In accordance with references (a) through (g), the following information is provided. On Saturday, December 10th, 2011 from 1800 to 2300 the Navy Tenant Command (NTC) will hold its annual holiday party at the Springfield Marriott. NTC expects participation to exceed 300 military, DOD civilian, and dependents. This event is limited to ticketed command personnel, in civilian dress, and is not open to the general public. This event has only been advertised within command communication channels (plan of the week, department head meetings, MWR representatives). NSF is not involved in the execution of this security plan.

a. Friendly Forces

- (1) Springfield Police Department (SPD)
- (2) Marriott Security Staff
- (3) Springfield Fire and Emergency Services (FIRE)
- (4) Intercity Life Flight (ILF)

b. Enemy Forces. See reference (a).

Enclosure (6)

31 MAR 2014

c. Threat Summary. NTC has conducted a risk assessment, reference (b), based on the information provided in reference (b). With due consideration to the current FPCON and the low profile of this event, a backpack IED or an active shooter scenarios are the most likely threats to this event.

d. Assumptions. The following assumptions were used in the development of this plan:

(1) The current FPCON will not change before execution of the event.

(2) This event is not publically advertised and is not actively being targeted.

(3) Participants will not be in uniform and therefore do not present a highly desirable target or an obvious DOD presence.

(4) The measures provided herein will project the image of a hard target to potential adversaries.

e. Mitigation Ability. NTC has worked closely with the NSS security department and NCIS in the development of this security plan. No current activity indicates criminal or terrorist surveillance and/or planning nor does reference (a) indicate any specific threats. NTC CO is confident that the security provisions outlined herein effectively mitigate potential risks to NTC personnel and is comfortable that this event does not present any appreciable risk.

2. Mission. Coordinate with local law enforcement and Marriott security to provide a secure environment for the NTC holiday party. Mission objectives are as follow:

a. Provide a safe and secure environment.

b. Deter and detect terrorist and criminal threats.

c. Should an event occur, mitigate the effects of a terrorist or criminal act.

d. Should an event occur, recover from a terrorist or criminal act.

3. Execution

31 MAR 2014

a. Commander's Intent. Ensure security provisions provide a sufficient level of protection to counter the known and anticipated threats to command personnel and to mitigate potential high risk threats identified by the risk assessment, reference (b).

b. This plan outlines three phases of operations.

(1) Phase 1 - The planning and coordination outlined herein constitute this phase.

(2) Phase 2 - Execution of the event and this plan.

(3) Phase 3 - Return the installation to normal baseline force protection posture and capture any lessons learned.

c. Task Organization. The following outlines the participating organizations and their assigned roles:

(1) Navy Tenant Command:

(a) Prepare risk assessment, reference (b), and coordinate with local law enforcement and the Marriott staff to ensure adequate security provisions are made to mitigate potential threats.

(b) Command MWR representatives will collect tickets and validate all participant identification for entry into the party.

(c) Event Staff will limit baggage into the event to small handbags. All participants have been briefed and ticket collectors will require any person with a large bag to return the bag to their vehicle.

(2) Springfield Police Department (SPD). SPD will provide the following:

(a) SPD Supervisor. One site supervisor will be available to liaison with SPD dispatch to obtain back-up for security incidents that exceed the capability of the on-site law enforcement personnel.

(b) Entry Control. One officer will be stationed in the area of the entry point to the party to assist event staff in handling persistent attempts to gain unauthorized access.

31 MAR 2014

(c) Security Patrol. One officer will patrol within the designated perimeter of the holiday party.

(d) K-9 Sweep. SPD Special Operations Unit will sweep the event location prior to the event and station the roving patrol on-site to maintain site integrity.

(e) Fully describe other security provisions of LLE.

(3) Marriott Hotel Security:

(a) Establish event perimeter with partitions and red ropes.

(b) Monitor hotel security cameras and report suspicious activity to the SPD supervisor.

(c) Fully describe any other security provisions

4. Administration and Logistics

a. Pre-Planned Responses. Attendees will be briefed on emergency situations during the opening remarks of the party. See enclosure (4) for specific response actions.

b. NTC MWR is the sponsoring organization for this event. All requests for event logistics support will be submitted to NTC MWR Representative, Mr. Ho-Lee Kow (888-555-1234).

5. Command and Control

a. The SPD Supervisor will exercise command and control for the security of this event. Marriott Security will participate in a subordinate role and refer all security related incidents to SPD.

b. Communications

(1) SPD Primary: Channel-1

(2) SPD Alternate: Channel-2

(3) Marriott Security: Hotel 1VBPD Dispatcher

Commanding Officer Signature

31 MAR 2014**Sample SEAT submission template - On Base (Small)**

CLASSIFICATION - (dependant on enclosures)

From: Commanding Officer, Navy Tenant Command
To: Commanding Officer, Host InstallationSubj: SPECIAL EVENT ANTITERRORISM PLAN - SPECIAL ACCESS
VISITORSRef: (a) (S) NCIS Threat Assessment (Date)
(b) (S) Event Specific Risk Assessment
(c) NAVSTA SPRINGFIELD OPOD AT-3300
(d) DoDI 2000.16
(e) (S) COMUSFLTFORCOM OPOD 3300 (Series)
(f) USFF Force Protection (FP) Directive 11-009 (111900Z
MAY 11)
(g) COMNAVREGMIDLANT OPPRD-AT 3300.1Encl: (1) Event Layout
(2) Watchbill - NSS NSF Additional Watches
(3) Emergency Plans and Notification Matrix
(4) Event Invitation

1. Situation. In accordance with references (a) through (g), the following information is provided. On Saturday, 4 July 2013 from 1800 to 2300 the Navy Tenant Command (NTC) Commanding Officer will host a Fourth of July barbeque at the CO's on base residence. Participation is limited to 85 invited guests and will include prominent members of the local community, senior military and DOD civilian's, and dependents. Guests will be in possession of an invitation, see enclosure (4). This event has not been advertised and knowledge of this event is not public knowledge.

a. Friendly Forces

- (1) Naval Station Springfield Security Force (NSF)
- (2) Naval Station Springfield Fire and Emergency Services (FIRE)

b. Enemy Forces. See reference (a).

c. Threat Summary. NTC has conducted a risk assessment, reference (b), based on the information provided in reference (a).

Enclosure (7)

3 1 MAR 2014

With due consideration to the current FPCON, the low profile, and the invitation only status of this event a backpack IED or an active shooter scenario is the most likely threat to this event.

d. Assumptions. The following assumptions were used in the development of this plan:

(1) The current FPCON will not change before execution of the event.

(2) This event is not publically advertised and is not actively being targeted.

(3) Participants will be within the protected perimeter of the installation and will not visibly increase potential target desirability.

e. Mitigation Ability. NTC has worked closely with the Naval Station Springfield (NSS) security department and NCIS in the development of this security plan. No current activity indicates criminal or terrorist surveillance and/or planning nor does reference (a) indicate any specific threats. NTC CO is confident that the security provisions outlined herein effectively mitigate potential risks to NTC personnel and is comfortable that this event does not present any appreciable risk.

2. Mission. Coordinate with NSS for overall situational awareness and to provide a secure environment for the NTC bar-b-que. Mission objectives are as follow:

a. Provide a safe and secure environment.

b. Deter and detect terrorist and criminal threats.

c. Should an event occur, mitigate the effects of a terrorist or criminal act.

d. Should an event occur, recover from a terrorist or criminal act.

3. Execution

a. Commander's Intent. Ensure security provisions provide a sufficient level of protection to counter the known and anticipated threats to command personnel, invited guests, and

31 MAR 2014

family members to mitigate potential high risk threats identified by the risk assessment, reference (b).

b. This plan outlines three phases of operations.

(1) Phase 1 - The planning and coordination outlined herein constitute this phase.

(2) Phase 2 - Execution of the event and this plan.

(3) Phase 3 - Return the installation to normal baseline force protection posture and capture any lessons learned.

c. Task Organization. The following outlines the participating organizations and their assigned roles:

(1) Navy Tenant Command:

(a) Prepare risk assessment, reference (b), and coordinate with NSS staff to ensure adequate security provisions are made to mitigate potential threats.

(b) NTC Protocol Officer will collect tickets and validate all participant identification for entry into the party.

(c) NTC Operations Officer (OPS) will identify and assign personnel to maintain a liaison at NSS gate 2 with a list of invited guests to coordinate with NSS security for questions, directions, and resolution of any guests that may have forgotten their invitation. NTC OPS will coordinate with NSS NSF for a handheld radio to communicate with security as necessary.

(d) NTC PAO will ensure the designated route from NSS gate 2 to the commander's residence is identified with directional signage.

(e) Ensure invitations instruct guests to limit baggage to small handbags.

(2) NSS NSF will provide the following:

(a) Traffic Control. NSF will provide a limited route to flag officer housing using cones and barriers with one patrol officer at the intersection of Nimitz St. and Ashland Ave to allow all other authorized traffic into the remainder of the installation.

31 MAR 2014

(b) Entry Control. NSS will control access to the installation via standing NSS SOP with the exception of allowing invited guests into the controlled route to flag officer housing.

(c) Security Patrol. NSS NSF will increase the periodicity of patrols in the vicinity of flag officer housing during the period of the event.

(d) Communications. NSS NSF will provide a handheld radio to NTC OPS for use as a primary response communication method.

(e) Fully describe any other security provisions applied.

4. Administration and Logistics.

a. Pre-Planned Responses. NTC staff has been briefed on the relevant portions of the NSS PPRs and event specific emergency evacuation plans. NTC Staff will be readily identifiable by bright yellow event shirts and will provide direction to guests as necessary during emergency situations.

b. NTC PAO is the NTC coordinator for this event. All requests for event logistics support will be submitted to, Mr. Ho-Lee Kow (888-555-1234).

5. Command and Control.

a. The NTC Operations Officer is the designated representative to coordinate with the NSS Security Officer for any required security response. NSS Commanding Officer, or a designated representative, will exercise command and control for responding NSF.

b. Communications

(1) NSF Primary: Channel-1

(2) NSF Alternate: Channel-2

(3) Telephone

Commanding Officer Signature