From: Commander, Navy Reserve Forces Command

Subj: ANTI-TERRORISM/PHYSICAL SECURITY PLAN FOR COMMANDER, NAVY RESERVE FORCES COMMAND, BUILDING NH-32

Ref: (a) DoD Instruction 2000.16 of 17 Nov 2016, Volume 1 and Volume 2
(b) OPNAVINST 3300.53C (FOUO)
(c) OPNAVINST 5530.14E CH-2
(d) NSA OPORD AT-3300-09
(e) USPACOM OPORD 5050-08 (FOUO)
(f) DoD Directive 4500.54E of 28 Dec 2009
(g) USNORTHCOM INST 10-222

Encl: (1) Anti-Terrorism and Force Protection
(2) COMNAVRESFORCOM FPCON and Physical Security Plan
(3) Barrier Plan/Exterior Building Drawing
(4) Emergency Action and Evacuation Plans
(5) Telephonic Threat SOP
(6) Visitor SOP
(7) Camera System SOP
(8) Lenel Alarm Monitoring System SOP
(9) Building NH-32 Alarm Actions
(10) 100% ID/Bag Check SOP
(11) Unauthorized Items
(12) Staff Active Shooter Responses
(13) Command Duty Pre-Planned Responses
(14) Radio Communication SOP
(15) Individual Anti-Terrorism Travel Plan
(16) Loss Prevention Plan

1. **Purpose.** Provide Anti-Terrorism (AT) and Physical Security policy and guidance for Commander, Navy Reserve Forces Command (COMNAVRESFORCOM), building NH-32, located onboard Naval Support Activity Hampton Roads (NAVSUPPACT HR), per references (a) through (g). Enclosures (1) through (16) provide detailed guidance concerning the AT/Force Protection (FP), Physical Security Plan and AT/FP guidance concerning travel outside of the United States per reference (f).

2. **Cancellation.** COMNAVRESFORCOMINST 3300.2A.
3. **Scope and Applicability.** This instruction establishes the AT/FP and Physical Security Plan for COMNAVRESFORCOM. This instruction will act as an addendum to NAVSUPPACT HR instructions and provide specific instructions to COMNAVRESFORCOM personnel in emergency situations. This instruction is applicable to all staff personnel and visitors to COMNAVRESFORCOM, building NH-32

4. **Action.** The designated Anti-Terrorism Officer (ATO) will be the point of contact for all command anti-terrorism and physical security issues. All assigned members of the command will be familiar with the contents and requirements of this instruction.

5. **Records Management.** Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.

5. **Review and Effective Date.** Per OPNAVINST 5215.17A, COMNAVRESFORCOM ATO will review this instruction annually on the anniversary of the effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date, or an extension has been granted.

\[\text{Signature}\]

L. D. STUFFLE
Chief of Staff

Releasability and distribution:
This instruction is cleared for public release and is available electronically only via COMNAVRESFOR Web site, [https://www.navvreserve.navy.mil](https://www.navvreserve.navy.mil)
ANTI-TERRORISM AND FORCE PROTECTION

1. **Purpose.** Provide information on Crisis Management Procedures in the event of a terrorist attack or threat.

2. **Responsibilities**
   
   a. The Commanding Officer, NAVSUPPACT HR is responsible for the maintenance of law and order within the grounds and buildings of NAVSUPPACT HR. To enforce this authority, the Commander may take necessary military actions to protect life in the event of a sudden and unexpected terrorist attacks or other emergencies disrupting the normal process of government. As a tenant, COMNAVRESFORCOM will follow the guidelines set by the host activity. Reference (d) provides AT guidance and policy for NAVSUPPACT HR tenant commands.

   b. Experience has shown that alertness, coupled with common sense and personal initiative in taking security precautions, is the best deterrent to terrorist situations. NAVSUPPACT HR has established programs that will:

   (1) Provide ongoing terrorist awareness training.

   (2) Coordinate AT/FP actions with other installations, Mid-Atlantic regional and tenant commands.

3. **Force Protection Conditions (FPCON)**

   a. FPCON warnings are the principle means a Commander has to apply an operational decision on how to guard against a threat. They provide a management system that is adaptable to a full spectrum of security needs from minor civil disturbances to general war. These conditions will be employed to the extent required to provide the degree of security considered appropriate for the existing threat.

   b. Reference (d) provides specific FPCON measures for tenants located on NAVSUPPACT HR.

   c. Further discussion on FPCONs and Threat Levels can be found in enclosure (2) of this instruction.

4. **Random Anti-Terrorism Measures (RAMs)**

   a. RAMs are used to enhance local FPCON measures. The implementation of RAMs provides the following:

   (1) Serves as a tool to enhance the security of installations and tenant commands.

Enclosure (1)
(2) Changes the security atmosphere within the installation. Such programs, when implemented in a truly random fashion, alter the external appearance or security “signature” of the installation to would-be terrorists and their supporters who may be providing surveillance assistance.

b. RAMs are procedures that are normally executed at specific FPCON levels. At any given level, implementing certain measures from a higher Force Protection Condition conveys an impression of increased vigilance and awareness to observers.

c. Reference (d) addresses the RAM program on NAVSUPPACT HR.

d. COMNAVRESFORCOM (N3AT) will manage and maintain a local RAM plan for COMNAVRESFORCOM Headquarters.

e. COMNAVRESFORCOM Command Duty Officers (CDO) are responsible for executing physical security RAM for specific FPCON levels.

5. Installation and Facilities Access

a. Because COMNAVRESFORCOM is a tenant, installation access is governed by requirements contained in reference (d).

b. Enclosure (6) provides direction for visitor access control of the COMNAVRESFORCOM Headquarters Building NH-32.

6. AT Training

a. AT Level I, II, III and IV training requirements are found in references (a) and (b).

b. Training objectives are to promote AT awareness, develop and identify personnel who have complied with annual Level I training requirements.

c. The COMNAVRESFORCOM ATO will ensure that all assigned military and civilian personnel receive Level I Anti-terrorism Awareness training annually, as required.
COMNAVRESFORCOM FPCON AND PHYSICAL SECURITY PLAN

1. **Purpose.** To integrate available forces, equipment, and procedures into an effective AT/FP and physical security plan for the protection of COMNAVRESFORCOM assets.

   a. **Concept.** Security for building COMNAVRESFORCOM is designed to ensure positive detection, identification, interception, and prevention of any unauthorized access to NH-32.

   b. **Security objectives.** The overall objective of the AT/FP and physical security plan is to protect national security interests against actions by adversaries, both foreign and domestic, in order to establish effective priorities. The security objectives of building NH-32 are:

      (1) **Primary Objectives.** The primary security objectives are to provide a security system that will:

         (a) Prevent unauthorized access to building NH-32.

         (b) Prevent theft or compromise of classified information or assets.

         (c) Protect and prevent loss of life.

      (2) **Secondary Objectives.** Ensure the safety of both persons and property through the use of access controls, internal circulation restrictions and personnel identification procedures.

   c. **Terrorist Threat Assessment.** The Naval Criminal Investigative Service Naval Station Norfolk Office provides periodic threat assessments upon request or due to changing threat conditions. The assessment will include building NH-32 and the area surrounding the facility. The threat assessment will be used to ensure the security plan remains current and reflects any threat or vulnerability discerned at that time.

2. **Area Security.** The following restricted areas are designated in building NH-32:

   a. **Level One:**

      | ROOM NUMBER | DESCRIPTION          |
      |--------------|----------------------|
      | 118/118A/118B/118C | DUTY OFFICE          |

   b. **Level Two:**

      | ROOM NUMBER | DESCRIPTION          |
      |--------------|----------------------|
      | 114A         | EKMS VAULT           |
      | 115/115B     | SIPR CAFÉ            |
      | 217          | TELCOM CLOSET        |

Enclosure (2)
3. **Force Protection Control Measures.** FPCON measures specify the actions commanders require to counter the threats of terrorist attacks, hostile acts, and hostile adversaries. The DoD FPCON system includes FPCON NORMAL mandatory measures, FPCON ALPHA through DELTA mandatory measures, and GCC-directed FPCON NORMAL through DELTA supplemental measures. A list of these FPCON measures are located in reference (a), Volume 2 and reference (g), attachment 2. Additionally, site-specific FPCON measures are maintained by the ATO.

4. The CDO will implement required FPCON measures as prescribed by NAVSUPPACT HR in coordination with the ATO.
BARRIER PLAN/EXTERIOR BUILDING DRAWING

1. General. Physical barriers control, deny, impede, delay, and discourage access to restricted and non-restricted areas by unauthorized personnel. Properly posted physical barriers are a must in the prosecution of intentional trespassers. The perimeter may be natural or man-made. Where the perimeter is a fabric fence, it will meet the standards and security requirements stated in reference (c). Where the perimeter is a masonry or similarly constructed wall, it will meet the requirements of reference (b). Where "natural" barriers are used, they will provide substantial difficulty in traversing to be actually considered a barrier. For example, clearly navigable and regularly used waterways will not be considered a "natural barrier."

2. Barriers. Barriers such as bollards, walls, gates, and berms will be constructed and employed to provide the maximum protection needed for the risk level associated with the targeted asset. The following guidance is established:

   a. Ensure that barrier plans protect critical assets and perimeter/entry control points from the design basis threat.

   b. All permanent-type barrier construction will be approved by the ATO and Chief of Staff (COS).

   c. Barrier deployment will be coordinated with the COS and ATO.

   d. Deployment of barriers will be used to support the physical security of Building NH-32 during heightened FPCONs.

   e. Barriers deployed in roadways will:

      (1) Not be deployed in installation roadways without NAVSUPPACT HR's approval.

      (2) Not be deployed in a manner to create a safety hazard for vehicles or pedestrians.

      (3) Be painted with fluorescent or reflective markings.

      (4) Unmanned barriers will be employed in a manner to allow vehicle operators safe rerouting alternatives. Further, other warning devices such as signs and reflective cones will be employed in conjunction with the barrier to provide vehicle operators ample warning/reaction time.

      (5) Plastic-type water barricades will be anchored in place with sufficient quantities of water to provide stopping power and prevent barriers from being driven by the wind.
3. **COMNAVRESFORCOM Barrier Plans**

   a. The barrier plan will be implemented during periods of increased FPCON in order to limit access to COMNAVRESFORCOM parking lot and parking garage and reduce the ability of Vehicle Borne Improvised Explosive Device penetration to COMNAVRESFORCOM facilities/areas and to present another security perimeter. The plan provides specific details regarding the placement of vehicle barriers during each FPCON.

   b. The barrier plan will reduce the volume of vehicle and pedestrian traffic entering/leaving.

   c. Implementation of the barrier plan will be directed by the COS and linked to the installation FPCON system.

   d. The barriers for COMNAVRESFORCOM Building NH-32 will be supplied and stored by NAVSUPPACT HR. The barriers will be placed during FPCON CHARLIE by Public Works and NAVSUPPACT HR security. While setting FPCON Charlie, COMNAVRESFORCOM will direct all nonessential personnel to depart the area. Security personnel and watchstanders will remain (at a minimum) until Building NH-32 is secure. A total of six individual barriers will be used to implement the COMNAVRESFORCOM barrier plan. Two barriers will be placed at the north end and two barriers will be placed at the south end of the parking lot entrances. One barrier will be placed at the north entrance and one barrier will be placed at the south entrance to the access road for deliveries on the west side of the building. See exterior drawing building placement.
EMERGENCY ACTION AND EVACUATION PLANS

Emergency Action Plan

1. Emergency Action Plan (EAP) will be posted in every COMNAVRESFORCOM Departments access doors and the appropriate POC will be updated and maintained by the appointed NH-32 Facility Fire Marshall. See EAP placard below.

2. The below EAP placard applies to all COMNAVRESFORCOM/CNAFR Codes in NH-32 facility.

---

CNRFC Emergency Action Plan (NH-32)
1912 Forrester Drive, Norfolk, Virginia 23551-6611

Emergency: 444-3333

SECTION I - EMERGENCY ORGANIZATION INFORMATION

<table>
<thead>
<tr>
<th>ORGANIZATION CONTACT</th>
<th>OFFICE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCOS:</td>
<td>(757)</td>
</tr>
<tr>
<td>LCPO:</td>
<td>(757)</td>
</tr>
</tbody>
</table>

SECTION II - EMERGENCY PREPAREDNESS GUIDANCE

<table>
<thead>
<tr>
<th>FIRE OR SMOKE</th>
<th>UTILITY FAILURE/POWER LOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Notify Fire Department at 444-3333</td>
<td>1. Notify CDO/N4/NAVFAC.</td>
</tr>
<tr>
<td>2. Activate fire alarm to evacuate building utilizing the nearest EXIT (Muster in designated areas; conduct accountability of Staff personnel; and provide must report to CDO)</td>
<td>2. Verify generator is online</td>
</tr>
<tr>
<td>3. Re-enter building ONLY when given &quot;all clear&quot;.</td>
<td>3. Turn off Unnecessary Equipment</td>
</tr>
<tr>
<td>4. Establish RAM watch</td>
<td>4. Establish RAM watch</td>
</tr>
<tr>
<td>5. Telework will be COS description</td>
<td>5. Telework will be COS description</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>THREAT (Bomb, Chem/Bio/Suspicious Package)</th>
<th>DISASTER/TROPIC OR WINTER WEATHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Record information on Telephonic Threat Complaint Form and dial &quot;57&quot; to trace the call if disconnected.</td>
<td>1. CDO/Emergency Management will notify personnel of disaster/weather either by Internal or external means.</td>
</tr>
<tr>
<td>3. Activate fire alarm to evacuate building utilizing the nearest EXIT (Muster in designated areas; conduct accountability of Staff personnel; and provide must report to CDO).</td>
<td>3. Activate Recall as directed</td>
</tr>
<tr>
<td>4. DO NOT search, assess, or touch: bomb/biological/chemical objects or suspicious package.</td>
<td>4. Mass communication if Essential Personnel (Duty Section) only authorized on Base.</td>
</tr>
<tr>
<td>5. Re-enter building ONLY when given &quot;all clear&quot;.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACTIVE SHOOTER</th>
<th>TORNADO/SEVERE WEATHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Notify CDO and call 444-3333</td>
<td>1. CDO/Emergency Management will notify personnel of tornado/severe weather either by Internal or external means.</td>
</tr>
<tr>
<td>2. If able to Evacuate (Run):</td>
<td>2. Do not exit out to the open and remain inside the facility</td>
</tr>
<tr>
<td>Have an escape route and plan in mind.</td>
<td>3. Shelter at the central lowest level/floor away from windows/doors and protect your head in any means necessary.</td>
</tr>
<tr>
<td>3. If unable to Evacuate (Hide):</td>
<td>4. Provide muster to the CDO when able.</td>
</tr>
<tr>
<td>Hide in an area out of the shooter’s view Block entry to hiding place and lock doors Silence cellphones</td>
<td></td>
</tr>
<tr>
<td>Turn off lights/cover windows</td>
<td></td>
</tr>
<tr>
<td>4. As last resort Take Action and only when your life is in imminent danger (Fight)</td>
<td></td>
</tr>
</tbody>
</table>

GENERAL EVACUATION PLANS FROM COMMANDER NAVY RESERVE FORCES COMMAND

EACH DEPARTMENT SHOULD Evacuate all Personnel, secure doors then proceed toward the designated area located across the NH-32 Front Parking lot and muster with your department.

Enclosure (4)
Emergency evacuation plan

1. Call Emergency Management Center 444-3333. Notify CDO.

2. Upon receiving direction from the CDO, sound the alarm via the PA system. If the direction is to evacuate the building, be sure to announce the muster location if different from the standard location.

3. CDO and SDPO ensure the building is empty.

4. Complete full muster of all personnel and report to CDO/Security.

5. Meet the responding unit at a designated location. COMNAVRESFORCOM CDO will contact the Base CDO at 438-3402 to arrange meeting.

6. Once security has arrived on scene, they will take over and follow their SOPs.

Emergency Evacuation Route

First Floor

[Diagram of the first floor showing evacuation routes and muster locations]
Muster Area
TELEPHONIC THREAT SOP

1. Complete the questions on the telephonic threat complaint form next to your phone.

   a. This SOP is designed to assist the user in getting as much information as possible when a telephonic threat is made. In accordance with the Basic Military Requirements, NAVAEDTRA 14325 and NTTP 3-07.2.3, each hard line will have a Telephonic Threat Complaint Form (OPNAV 5527/8) next to it.

   b. When a threat is received by telephone, the person taking the call should take the following actions:

      (1) Try to keep the caller on the line and obtain as much information as possible. Complete the Telephonic Threat Complaint form while the caller is on the line or immediately thereafter.

      (2) Record in writing the exact words of the caller.

      (3) Try to identify the location of the bomb, the type of device, what it looks like, and the expected time of detonation.

      (4) Attempt to determine the sex, approximate age, and attitude of the caller.

      (5) Note any background sounds that may provide clues to the caller's location.

      (6) Note any accent or peculiarity in speech that may identify the person.

2. Notify Emergency Call Center (ECC) at 444-3333 or 911.

3. If it is determined the threat is real, make an announcement and activate the fire alarm if necessary to evacuate COMNAVRESFORCOM, building NH-32.
# DEPARTMENT OF THE NAVY

## TELEPHONIC THREAT COMPLAINT

### IF BOMB THREAT, ASK THE CALLER
- WHEN IS THE BOMB TO GO OFF?
- WHERE IS THE BOMB TO GO OFF?
- WHAT KIND OF BOMB IS IT?
- WHAT DOES THE BOMB LOOK LIKE?
- WHERE ARE YOU CALLING FROM?

### 1. COMMAND

<table>
<thead>
<tr>
<th>a. Name &amp; Address</th>
<th>b. Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2. COMPLAINANT

<table>
<thead>
<tr>
<th>a. Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

### 3. PERSON RECEIVING CALL

<table>
<thead>
<tr>
<th>a. Name</th>
<th>b. Date &amp; Place of Birth</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>c. Command Name &amp; Address</th>
<th>d. Phone Number (Work)</th>
<th>(Home)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4. TELEPHONE CALL RECEIVED ON

<table>
<thead>
<tr>
<th>a. Phone Number (include area code)</th>
<th>b. Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>c. Phone Number Listed in (&quot;s&quot; all that apply)</th>
<th>d. Command Directory</th>
<th>e. Base Directory</th>
<th>f. Local Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>g. Unlisted</th>
<th>h. Other (list)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 5. DETAILS OF CALL

<table>
<thead>
<tr>
<th>a. Date</th>
<th>b. Day of Week</th>
<th>c. Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 6. CONTEXT OF CONVERSATION

<table>
<thead>
<tr>
<th>a. Recipient - &quot;</th>
<th>b. Caller - &quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>c. Recipient - &quot;</th>
<th>d. Caller - &quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>e. Recipient - &quot;</th>
<th>f. Caller - &quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 7. BACKGROUND NOISES (Describe street sounds, voices, music, etc. If more space is needed continue on reverse.)

### 8. INFORMATION ABOUT CALLER/VOICE CHARACTERISTICS

<table>
<thead>
<tr>
<th>a. Sex</th>
<th>b. Age</th>
<th>c. Race</th>
<th>d. Accent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>e. Educational Level</th>
<th>f. Attitude (calm, nervous, serious)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>g. Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

### 9. WERE THERE ANY WITNESSES TO THE CALL?  
[ ] No  [ ] Yes (List name)

### 10. DO YOU HAVE ANY SUSPICION AS TO THE IDENTITY OF THE CALLER?  
[ ] No  [ ] Yes (List name)

### 11. NOTIFICATION OF AUTHORITY ("s" all notified)

- [ ] CO
- [ ] XO
- [ ] OCD
- [ ] Security
- [ ] NISRA
- [ ] Telephone Company
- [ ] EOD
- [ ] Fire Dept

**OPNAV 5827-A . 12-42**  
SN 0107 LF-055-274B  
Enclosure (5)
VISITOR SOP

Business Hours

<table>
<thead>
<tr>
<th></th>
<th>Monday - Friday</th>
<th>Saturday - Sunday</th>
<th>Holidays</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0730 To 1630</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

1. **General.** This SOP is designed to inform the Duty Section(s) and Watch personnel of the proper procedures for building entry and visitor access to building NH-32. The procedures are set in conjunction with the FPCONs.

   a. **Information**

      (1) Working hours and alarms:

         (a) The normal working hours for COMNAVRESFORCOM are 0730 to 1630 Monday through Friday on non-holidays.

         (b) The normal working hours of the building NH-32 building entry system are 0630 to 1800 Monday through Friday on non-holidays.

      (2) Visitor Definition:

         (a) Visitor (Military/Civilian/Contractor) will show valid identification and prescreened by security (N01S) to gain access to COMNAVRESFORCOM. A visitor badge will be issued and displayed at all time. An escort is not required.

         (b) Restricted Visitor (Military/Civilian/Contractor/Dependent/Guest) will show valid identification, an escort is required at all times. A visitor badge will be issued and displayed at all time. The restricted visitor will not be prescreened by security (N01S).

      Note: Person of Interest (POI) (Military/Civilian/Contractor/Dependent/Guest) will be deny entry regardless of proper Identifications provided. Notify CDO/ATO or Base Law Enforcer Discretely to handle the situation.

      Note: After checking in with N01S, assigned personnel shall have a COMNAVRESFORCOM building NH-32 badge/access card.

   b. **Building Entry Procedures**

      (1) During normal working hours:
(a) Authorized personnel will have access through the COMNAVRESFORCOM badge system/swipe card access.

(b) Visitor access is granted by the SDPO after the visitor has provided positive identification and verified the access list for the event. The visitor will sign visitor log and no COMNAVRESFORCOM escort required.

(c) Restricted Visitor Access is granted by SDPO after positive identification has been verified and the COMNAVRESFORCOM/CNAFR POC has taken the responsibility of the individual and once visitor log has been signed by both parties (COMNAVRESFORCOM/CNAFR POC and visitor).

Note: Escort must be an COMNAVRESFORCOM/CNAFR personnel only.

(2) After Normal Working Hours:

(a) Authorized personnel have access through the COMNAVRESFORCOM badge system/swipe card access. After swiping their card they must enter their six digits Personal Identification Number (PIN) into the key pad.

(b) Restricted personnel/visitors are not granted access unless escorted by an authorized person(s), unless it is an emergency and access is authorized by the CDO.
CAMERA SYSTEM SOP

1. **General.** The Camera System SOP gives guidance on how to operate the COMNAVRESFORCOM, NH-32 camera system for security/safety monitoring. The SDPO will monitor and respond to safety in security threats.

2. **Procedures.** The person standing the duty will:

   a. Start the camera CPU.
   
   b. Go to the “Start” icon.
   
   c. Go to the “Security Desk” icon.
   
   d. Log on to the Video Camera Viewer by using the login username, password and directory IP address.
   
   e. Ensure the 24 inside video cameras appear on the left monitor and 10 outside video cameras appear on the right monitor.
   
   f. To maximize the video camera screen on both monitors, click on “Hide area view” and “Hide Dashboard” at the bottom left/right corner of each monitor.

3. **Retrieving video recording.**

   a. Right click on selected Video Camera.
   
   b. Select “Investigate”.
   
   c. Select “Camera Events”.
      
      (1) Select a “camera” you wish to view.
      
      (2) Select “Event Timestamp”.
      
      (3) Select “Event Recording”.
      
      (4) Click on “Generate Report”
      
      (5) When finished, click “X” on the top most tab of camera event.

Enclosure (7)
4. Turning off the camera CPU. This step will safely allow operator to turn off the camera CPU in case of maintenance or error while video recording capabilities will not be affected from the server.
   
a. Close the cameras main window by clicking on “X” on the top right corner of the right monitor.

b. Save the changes or disregard the setting.

c. Go to “Start” Icon.

d. Click on “Shutdown” Icon

5. Resetting the affected camera feed. This step will enable to restore the affected camera live feed from the server.
   
a. Right click on the selected camera

b. Select on “Camera”.

c. Click on “Select live stream”.

d. Select “Recording”.

e. Repeat step “5.a” to “5.a.2” and proceed to “5.a.5”.

f. Select “Live (Default)”.
LENEL ALARM MONITORING SYSTEM SOP

1. General. The purpose of the Lenel Alarm Monitoring System SOP is to inform, assist, and provide direction to the watchstanders on system start-up, operation, and end of work day procedures. Operating procedures will cover opening the front door for visitors, operating the exterior PTZ cameras, and watching recorded video from the Lenel Security Cameras.

2. Start Up Procedures
   a. At the beginning of the work day.
   b. Login to the Alarm Monitoring CPU.
   c. Go to the “Start” Icon.
   d. Go to “Programs”.
   e. Go to “OnGuard ET”.
   f. Click on “Alarm Monitoring”.
   g. Login to Lenel OnGuard Alarm Monitoring application by using the same login user name and password as the CPU.
   h. Ensure “access all segment assignments” is checked and then select “OK”.
   i. Click “OK” on the Alarm Monitoring Pop-up window that reads “No TCP/IP ports available for RPC server”.
   j. There should be two open windows including the “Main Alarm Monitor” and “System Status Tree (all devices)” windows. If the two windows are not open, click on the “yellow bells” icon and the “System Status Tree” icon at the top left hand side of the application.
   k. Click on the “System Status Tree (all devices)” tab at the bottom, left hand side of the application.
   l. Click on the “+” sign next to all of the system device icons in order to open them up.
   m. Click on all of the “+” signs next to all of the green squares with red dots. This opens up and displays all of the alarm sensors throughout the building.
   n. A red dot by the sensor means that the sensor is armed (unmasked). A grey dot means that the sensor is unarmed (masked).

Enclosure (8)
Monitor all of the device icons during the watch. If a red “X” appears on top of any device during the watch, the communication was lost with that sensor. Contact the CDO.

3. End of Work Day Procedures (Arming (Unmasking) the Spaces)

a. At the end of the work day, the custodians of the secure spaces will arm their respective spaces and report it to the SDPO on the Quarterdeck. The spaces that are to be secured and armed (unmasked) at the end of the work day, weekends, and holidays are:

   (1) The EKMS Vault, RM 114A

   (2) The SIPRNET Café, RM 115A and RM 115B

   (3) The 3rd Floor SCIF, RM 319

d. The SDPO must call NAVSUPPACT HR Security Dispatch (757) 836-1900 and Building NH-95 Security Desk (757) 836-5228, and inform that building watch has secured and that Sipernet Café and Sensitive Compartmented Information Facility are armed. Make log entry into the SDPO Log Book.

4. Monitoring Alarms

   a. Click on the “Main Alarm Monitor” tab at the bottom of the Alarm Monitoring application.

   b. All of the alarms that get activated and all of the door sensors that get triggered will get displayed on this screen.

   c. When an alarm or door sensor is triggered in a space that has been secured, notify the CDO immediately.

   d. When the alarm or door is noticed and the cause is known, then left click on the alarm.

   e. Click on the yellow check mark at the top of the application.

   f. Click “Yes” to acknowledge the selected alarm.
5. **Opening the front door for visitors**

   a. Go to the “System Status Tree (all devices)” tab at the bottom of the alarm monitoring application.

   b. Scroll down the device list until you see the “COMNAVRESFORCOM BUILDING NH-32 1ST FLOOR (Firmware revision: 3.064.aes)” device.

   c. Look for the “Main Entrance (access mode: card and PIN; masked: forced)” icon.

   d. Right click on this icon.

   e. Scroll up to “open door(s).”

   f. Left Click on it.

   g. The door will unlock for 3 seconds.

   h. Click the “OK” button on the Pop-up window signifying that you just activated the door lock.
BUILDING NH-32 ALARM ACTIONS

1. **General.** COMNAVRESFORCOM Headquarters Building NH-32 has several different alarm systems to assist the operations of the building. The alarm systems allow for central monitoring of building alarms. The duty section is required to be familiar with all alarm systems and actions if an alarm sounds. The types of alarms and procedures for responding to alarms follow.

2. **Types of building NH-32 Alarms:**
   
   a. **Sanitary Lift Station High Level Alarm** (set at 20 percent lift station level).
   
   b. **Emergency Diesel Generator Alarm Conditions** as indicated on the Emergency Diesel Generator remote indicating panel on the Quarter Deck.
   
   c. **Fire Alarm Supervisor’s Panel** (1MC outside the SDPO office on the Quarter Deck): Sounds a chirping alarm when a fault occurs in the system.
   
   d. **FM200 Fire Suppression Control Panel** for the Server Farm (RM 114): This panel is located outside the Server Farm door and is the indicating and alarm panel for the fire suppression system installed in the Server Farm room.

3. **Alarm Actions**
   
   a. **Sanitary Lift Station Alarm:**
      
      (1) Red Alarm on Quarter Deck (located behind SDPO watch on the wall): activates when lift station level reaches a high level-20 percent.
      
      (a) Acknowledge alarm by pushing alarm button behind SDPO watch on wall.
      
      (b) Make a 1MC securing the Heads.
      
      (c) Call the Public Works Trouble Desk: 445-6868
      
      (d) Acknowledge alarm by pushing the alarm reset at the Sanitary Lift Station located exterior to the front of the building on the gate side of the building.
      
      (e) Make log book entry.
      
      (f) Inform CDO.
      
      (2) Chirping alarm at the Sanitary Lift Station due to a loss of power.
(a) Acknowledge alarm by pushing the alarm reset at the Sanitary Lift Station located exterior to the front of the building on the gate side of the building.

(b) Inform the Public Works Trouble Desk: 445-6868

(c) Make log book entry.

(d) Inform CDO.

b. **Emergency Diesel Generator Alarms.** For any of the alarms mentioned above that indicate on the Emergency Diesel Generator remote Indicating Panel:

   (1) Read and record the alarm.

   (2) Call the Public Works Trouble Desk: 445-6868

   (3) Make log book entry.

   (4) Inform CDO.

c. **Fire Alarm Supervisor’s Panel chirping alarms.** For any alarm associated with the panel (except for expected alarms due to announcements):

   (1) Read and record alarm by reading the digital screen on the panel and recording the trouble fault displayed. The fault will be highlighted on the screen.

   (2) Call the Public Works Trouble Desk: 445-6868

   (3) Make log book entry.

   (4) Inform CDO.

d. **FM200 Fire Suppression Control Panel for the Server Farm (RM 114) alarms/trouble lights.** For any alarm associated with the panel (except for expected alarms due to announcements):

   (1) Read and record alarm by reading the digital screen on the panel and recording the trouble fault displayed. The fault will be highlighted on the screen.

   (2) Call the Public Works Trouble Desk: 445-6868.

   (3) Make log book entry.
100% ID/BAG CHECK SOP

1. General. 100% ID Check Plan is designed to control, deny, impede, delay, and discourage access to the COMNAVRESFORCOM NH-32 by unauthorized personnel during business hours (refer to Encl 6).

2. 100% ID/Bag Check Plan.

   a. The 100% ID/Bag Check Plan will be implemented during periods of increased FPCON or Authorized Random Anti-Terrorism Measures (RAMs) in order to limit access to the facility from unauthorized personnel and to impose another security measures.

   b. Implementation of the 100% ID/Bag Check will be directed by the COS or ATO, conducted as part of scheduled RAMs, or in response to increased installation FPCON Level as directed by NAVSUPACT HR.

   c. 100% ID Check Station is composed of a podium/stool, radio and CNRFC Command Duty Pre-Planned Responses Checklist; setup will be coordinated by the Master at Arms.

   d. Establish Radio communication to the Duty Desk and report “100% ID Check/Bag Inspection is now commencing”.

   e. “100% ID Check in progress” sign will be posted within each station to identify the location where to present the DOD CAC ID and COMNAVRESFORCOM building ID or a valid ID for the visitors to the watchstanders.

      (1) Any COMNAVRESFORCOM personnel that have degraded/severely faded or unreadable CNRFC ID will be logged in and escorted to Security for a replacement ID.

   f. 100% Bag Check will follow the same procedures as 100% ID Check with the following additions:

      (1) Back entrance will be secured and all foot traffic will be directed to the front entrance of COMNAVRESFORCOM.

      (2) Station conducting bag check will consist of an inspection table and be manned with an additional Duty MA to speed up the flow of personnel onto the Quarterdeck.

      (3) Personnel conducting the bag inspection will wear protective gloves and will utilize inspection device, such as 12 inch ruler, to prevent any direct contact with any potentially hazardous substances.

Enclosure (10)
(4) Direct the bag owner to move the items obstructing the inside view of every bag compartment.

(5) Notify the CDO/CMAA and always maintain control of any suspicious/unauthorized items found.

(6) Escort the individual who has the suspicious/unauthorized items to the waiting/holding area until proper authority is notified and assumes responsibility for the situation.

g. Each station will be manned by a Duty MA in the uniform of the day with cover and radio to establish communications to the CMAA.

h. Report to the SDPO “All Conditions Normal” every hour and “100% ID/Bag Inspection is secured” once the watch is ended.
UNAUTHORIZED ITEMS

1. **General.** Unless otherwise authorized by applicable law or regulation, the introduction of privately owned firearms, weapons, and fireworks, shall not be possessed, used, transported, or stored on board Commander Navy Reserve Forces Command Facility without prior written approval of Installation Commanding Officer (ICO). NSA Hampton Roads installations include; Naval Medical Center Portsmouth (NMCP), Northwest Annex, Camp Allen, SDA, and Lafayette River Annex.

2. **Unauthorized Items:**
   
a. **Firearms.** Any device that, when operated, propels an object (to exclude bows and arrows) or any device that produces a visible or audible effect by combustion, explosion, deflagration, or detonation, and shall include blank pistols, air guns, electrical weapons (stun guns, etc.) and ammunition.

   b. **Weapons.** Any object used, displayed, offered, or brandished in any manner to inflict or instill fear of inflicting bodily harm, or any object that by its very nature would be considered by a reasonable and prudent person to have been designed for the purpose of inflicting bodily harm (e.g., blackjacks, steel/brass knuckles, switchblade/stiletto knives (except common pocket knives with blades that do not exceed 3-1/2"), bows and arrows, crossbows, martial arts weapons, etc.)

   c. **Fireworks.** Any combustible or explosive composition or any substance or combination of substances; any article prepared for the purpose of producing a visible or an audible effect by combustion, explosion, deflagration, or detonation; blank cartridges and toy cannons in which explosives are used; firecrackers, skyrockets, Roman candles, Daygo bombs, and any fireworks containing flammable explosives, tablets, or other devices containing explosive substances.

   d. **Ammunition.** Includes projectiles with their fuses, propelling charges, and primers fired from guns, explosive military items (grenades, bombs), and any material used in an attack or defense.

   e. **Contraband.** Includes marijuana, cannabis, cocaine, heroin, alcoholic beverages, drug paraphernalia, etc.

3. **Exceptions.** The introduction or possession of any privately owned firearms or weapons on board NSA HR installations is strictly prohibited except for those listed below:

   a. **Law Enforcement**

   b. **Armored Car Guards**

Enclosure (11)
STAFF ACTIVE SHOOTER RESPONSES

1. **Purpose:** To address and delineate an SOP of an active shooter situation occurs at COMNAVRESFORCOM NH-32 or NSA, Hampton Roads.

2. **Discussion.** Active shooter situations are unpredictable and evolve quickly. Individuals must be prepared both mentally and physically to deal with an active shooter situation.

3. **Building Action.** CDO/Staff Duty Petty Officer (SDPO)
   a. Immediately secure any building entry access or lock all doors remotely via installed Lenel computer system at the duty desk if Active Shooter or Base initiates lock down.
   b. Notify the staff personnel of threat via announcing system or any communication device available.
   c. Notify the following as time/situation permits:
      (1) NSA Hampton Roads Police Dispatch at (757) 444-2324/(757) 836-1900 or (757) 444-3333/911.

**Notify law enforcement of the current situation and inform them of the threat.

(2) The COMNAVRESFORCOM Staff.

(3) Naval Criminal Investigative Service (NCIS) Regional Agency, (757) 444-7327.

4. **Staff member action**
   a. **Evacuate (Run).** If there is an accessible escape path, attempt to evacuate the premises. Be sure to:
      (1) Have an escape route and plan in mind.
      (2) Evacuate regardless of whether others agree to follow.
      (3) Leave your belongings behind.
      (4) Help others escape, if possible.
      (5) Prevent individuals from entering an area where the active shooter may be.

Enclosure (12)
(6) Keep your hands visible. If you encounter law enforcement, this will decrease the possibility of being mistaken for the shooter.

(7) Follow the instructions of any law enforcement personnel.

(8) Do not attempt to move wounded personnel.

b. Shelter/Barricade-In-Place (Hide). If evacuation is not possible, find a place to hide where the active shooter is less likely to find you.

(1) Choose a space out of the active shooter's view, provides protection if shots are fired in your direction (i.e., an office with a closed and locked door), and does not trap you or restrict your options for movement.

(2) To prevent an active shooter from entering your hiding place, positively shut and lock the door and/or blockade the door with heavy furniture. Confirm door is shut completely and locked.

c. Fight or Take action against the active shooter (Fight). As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:

(1) Acting as aggressively as possible against him/her.

(2) Throwing items and improvising weapons.

(3) Yelling.

(4) Committing to your actions.

d. Actions when law enforcement arrives (Comply). Law enforcement's purpose is to stop the active shooter as soon as possible. Law enforcement will proceed directly to the area in which the last shots were heard.

(1) Remain calm, and follow law enforcement instructions when shelter/barricade-in-place.

(2) Do not un-barricade unless it is confirmed that Law Enforcer has area cleared and it is safe to proceed.

(3) Put down any items in your hands (i.e., bags, jackets, mobile phones, etc.)

(4) Immediately raise hands and spread fingers.
(5) Keep hands visible at all times.

(6) Avoid making quick movements toward law enforcement such as holding on to them for safety and never point, scream or yell at them.

(7) Do not stop to ask law enforcement for help or direction when evacuating, proceed in the direction from which law enforcement are entering the premises.

e. When there is no longer a threat, the senior member present should engage in post-event assessments and activities, including:

(1) An accounting of all individuals at a designated assembly point to determine if anyone is missing and/or injured.

(2) Ensure chain of COMNAVRESFORCOM Staff has been notified.

(3) Determining a method for notifying families of individuals affected by the active shooter, including notification of any casualties.

(4) Assessing the psychological state of individuals at the scene, and referring them to health care specialists accordingly.

(5) Maintain a chronological log of events as they occur for incident reconstruction.

f. Activate COOP if the Facility are severely damage and impossible to return to normal working environment due to inaccessible because of extensive investigations and repairs.
# CNRFC Command Duty Pre-Planned Responses

**Emergency: 444-3333**

### 100% ID CHECK

1. Establish communication to the SDPO (Radio) and report "100% ID Check is commence".
2. Verify two form of ID (CAC and CNRFC Badge).
3. Log all personnel with ID discrepancy (Faded, Unreadable, etc.) via Duty Office for tracking and notify Command Services for re-issuance.
4. Escort visitor/personnel with/without any proper ID to the holding area until CNRFC POC will assumed responsibility.
5. Report to the SDPO "All Condition Normal" every hour and "100% ID Check is secured" once the watch is ended.

### BAG INSPECTION

1. Establish communication to the SDPO (Radio) and report "Bag Inspection is now commence".
2. Proper PPE is mandatory (Gloves/inspection device) for bag checker.
3. Instruct the bag owner to open/remove item that obstruct the inside view to all compartments of the bag.
4. Notify the CDO/CMMAA DISCRETELY for any suspicious items found and always maintain control of that item.
5. Escort the suspicious personnel to the front entrance waiting area until proper authority is notified and will assume responsibility.
6. Report to the SDPO "All Condition Normal" every hour and "Bag Inspection is secured" once the watch is ended.

### UNAUTHORIZED ITEMS

- Firearms
- Weapons
- Fireworks
- Ammunition
- Contraband
- Exception: Law Enforcement/Armored car Guards

### PERSON OF INTEREST (POI)

1. CDO/SDPO review the daily list of the POI.
2. State the purpose and document the POI visit.
3. Deny access to POI and notify CDO/ATO.
4. Contact the Base police if the POI refuse to leave the premises.

### VISITOR

1. Business Hours:
   - Weekdays: 0730 to 1630
   - Weekends: Not Applicable
2. Grant visitor access and provide appropriate visitor badges when he/she provided proper ID and CNRFC escort assumed responsibility after they signed visitor log.
3. SDPO will track/conduct visitor badges inventory before the end of a business hours.

### THREAT (Bomb, Chem/Bio/Suspicious Package)

1. Record information on Telephonic Threat Complaint Form and dial "57 to trace the call if disconnected.
2. CDO will notify the Security.
3. Activate fire alarm to evacuate building. Muster in designated areas and conduct accountability muster of Staff personnel and provide it to CDO.
4. DO NOT search, assess, or touch: bomb/biological/chemical objects or suspicious package.
5. Re-enter building ONLY when given "all clear".

## GENERAL COMMAND DUTY PRE-PLANNED RESPONSE FROM COMMANDER NAVY RESERVE FORCES COMMAND

**EACH DUTY SECTION SHOULD**

Informed/Protect all Staff Personnel in any safety/hazard known situation in NH-32 facility.

(Front)

Enclosure (13)
# CNRFC Command Duty
## Pre-Planned Responses

<table>
<thead>
<tr>
<th>1915 Forrestal Drive, Norfolk, Virginia 23551-4615</th>
<th>Duty Office: 757-445-8500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency: 444-3333</td>
<td>CDO Phone: 757-274-9554</td>
</tr>
<tr>
<td><img src="" alt="Table" /></td>
<td>SDPO Phone: 757-282-1276</td>
</tr>
</tbody>
</table>

### FIRE OR SMOKE
1. Notify Fire Department at 444-3333 or 911.
2. Sound the Fire Alarm System and announce the muster location if different from designated location.
3. CDO/SDPO coordinate with the Fire Department as required.
4. Make a full muster of all personnel and report to CDO.
5. Re-enter ONLY when notified that the building is safe by Fire Marshall.

### DISASTER/TROPIC OR WINTER WEATHER
1. Emergency Management will notify personnel of disaster/weather either by Internal or external means.
2. CDO will review Emergency Management Plan/Carry out actions outlined in COOP Instruction.
3. CDO will make announcement to send personnel home and telework is authorized with DCOS discretion.
4. CDO/SDPO verify if building is empty and all doors are closed.
5. Activate Phone Tree recall as directed.

### ACTIVE SHOOTER
1. Secure all doors access as applicable and notify CDO, ATO and Staff personnel of threat.
2. CDO/SDPO notify Base Security at 444-3333 or 911.
3. Evacuate (Run)
4. Shelter/Barricade-In-Place (Hide)
5. Take action against active shooter as last resort (Fight)
6. COC/CDO will engage in post-event assessment and activities when there is no longer a threat.
7. CDO will generate a muster to determine if anyone is missing/injured and notify COC.

### UTILITY FAILURE/POWER LOSS
1. CDO will acknowledge triggered alarms.
2. CDO will contact NAVFAC and verify if generator is online.
3. Turn off all Unnecessary Equipment
4. Establish watchstanders at the Front/Back entrance of the Facility until the duration of the Utility Failure/Power Loss.
5. CDO will make announcement to send personnel home and telework is authorized with DCOS discretion.
6. Activate a 24 hour Watchbill at the Duty Desk for full coverage with 2 man rule for safety.
7. CDO will notify the Command once Utility/Power is restored and return the facility to Normal working environment.

### TORNADO/SEVERE WEATHER
1. CDO will notify personnel of tornado/severe weather either by Internal or external means.
2. Do not exit out to the open and remain inside the facility.
3. Shelter at the central lowest level/floor away from windows/doors and protect your head in any means necessary.
4. Provide muster to the CDO when able.

### SECURITY SYSTEM FAILURE
1. Notify the CDO/ATO and the Base Security.
2. Establish watchstanders at the Front/Back entrance of the Facility during normal working hours until the duration of the security system failure.
3. Activate a 24 hour Watchbill at the Duty Desk for full coverage with 2 man rule for safety.
4. CDO will notify the Command and secured the watchstanders once Security System is restored.

### GENERAL COMMAND DUTY PRE-PLANNED RESPONSE FROM COMMANDER NAVY RESERVE FORCES COMMAND
EACH DUTY SECTION SHOULD
Informed/Protect all Staff Personnel in any safety/hazard known situation in NH-32 facility.

(Back)

2 Enclosure (13)
RADIO COMMUNICATION SOP

1. **Purpose.** To establish a quick/fast/rapid mass communication and as a tool in enhancing security measures of the Duty Section personnel within the premises of the COMNAVRESFORCOM NH-32 facility in an event of any emergency situation. Be cautious of radio communications during a bomb threat or suspicious item.

2. **Responsibilities**
   
   a. ATO/AATO will be the overall monitor in maintaining radio inventory that will be issued or utilized within the command ensuring all radios are good working condition.

   b. Radios will be issued to and be carried by the following:
      
      (1) Front Office (CNRFC Flag Writer)
      
      (2) CDO
      
      (3) ATO/AATO
      
      (4) Chief MA
      
      (5) SDPO
      
      (6) RAM watchstanders

   b. CDO will determine the radio channel that will be utilized for the Duty section to deter any routine radio traffic as possible.

   c. CDO will verify/check radios condition as part of the duty turnover. Notify ATO/AATO if radios have any discrepancies.

   d. Front Office, Chief MA, SDPO and RAM watchstanders will ensure all radios will be fully charge prior in use.

   e. SDPO will log all the check-out/check-in process of all the radios being utilized or issued to personnel for tracking purposes. All radios will be returned to the duty desk to be inspected from any discrepancies and charge the battery after the end of business hours. Any discrepancies with the radios will be noted degraded/OOC to the radio log book status block.
INDIVIDUAL ANTI-TERRORISM TRAVEL PLAN

1. General. The IATP is required by references (e) and (f). This travel requirement has been in effect since 1999 for travel to the Pacific Command Area of Responsibility (AOR) and for other AORs as depicted in the Foreign Clearance Guide. It can be filled out by going to the following link: https://iatp.pacom.mil/.

2. Key Notes

   a. The IATP is not a document to approve travel. It is intended to be used in conjunction with an approved travel process.

   b. Your chain of command should have already approved your travel prior to the submission of an IATP request.

   c. The IATP routing process intentionally has a limited routing process and does not support multi-chops through the chain of command.

   d. The IATP was never intended to replace the formal methods of approving travel.

   e. The IATP should be submitted outside of the required timelines for a Travel Clearance Message, if one is required to your destination. See the DOD Foreign Clearance Guide for requirements. Link: https://www.fcg.pentagon.mil/fcg.cfm.

   f. The Travel Clearance Request is not part of this document. If required, it must be submitted in Aircraft and Personnel Automated Clearance System (APACS) after your IATP is approved. Link: https://apacs.dtic.mil/apacs/login.jsp.

3. The intended sequential process for travel is:

   a. Approval of travel through your chain of command.

   b. Obtain AOR location Specific Brief.

   c. Complete Level 1 ATFP Awareness Training.

   d. Complete SERE level B Code of Conduct Training.

   e. Submit Isolated Personnel Report (ISOPREP) and have it validated within Personnel Recovery Mission Software (PRMS).

   f. If going to Korea, complete USFK Required Training.
g. Submit an IATP and have it approved at the required level.

h. Submit Travel Clearance Request and have it approved within APACS.

4. Medical screening for OCONUS travel of recreation or other non-duty related reason will go to Naval Medical Center Portsmouth Traveler’s Health Clinic. This clinic will provide preventive health services and education to minimized health risks during OCONUS travel to specific locations.

   a. Please schedule your appointment at 757-953-5179 or 757-953-7005. Walk-in will not be accommodated.

Individual AT Plan Review Checklist

COMMUNICATIONS
☐ Availability of telephones in country (public/other) listed?
☐ Emergency telephone numbers for the (units in area to be visited) included?
☐ Contact phone numbers in country? (American Embassy/Consulate, U.S. Military, MP’s, Local police, fire, etc?)
☐ Contact numbers for use as an alternate source of obtaining threat info? (USPACOM JOC Director: 808-477-7377 or JIOC 2 SWC: 808-477-8173)

AMERICAN EMBASSY/CONSULATE LOCATIONS
☐ Street address and any other pertinent directions to locate the nearest American Embassy or Consulate available? (Links to all American Embassy web pages are available at the following website: http://www.usembassy.state.gov)

EMERGENCY ACTION PLANS
☐ Evacuation plans (Have emergency telephone numbers and points of contact to change airplane reservations, if required, been provided?)
☐ Does the plan include a statement that if suspicious activity possibly endangering personnel, facilities, or residences is identified, (Rank/Name) will notify hotel security, local police, MP’s or U.S. Military Intelligence as appropriate? If warranted, subsequent notification will be made to the USPACOM JOC Director at 808-477-7377?
☐ Does plan indicate locations of safe havens?
☐ Does plan address actions to take in the event of:
   1. Terrorist attack on hotel?
   2. Terrorist attack against workplace?
   3. Mob violence or civil disturbance in the (deployed location)?
   4. New terrorist threat information, change in Threat Level or FPCON?
   5. Natural disaster occurs in area of operations?

PERSONNEL RECOVERY
☐ Validation that SERE 100 Code of Conduct Level B training has been completed?
☐ Validation that ISOPREP data for all traveler(s) stored in the Personnel Recovery Management System (PRMS)?
☐ HQ USPACOM 3JS Personnel Recovery/SERE 100 Code of Conduct POI info provided?
   - Mr. Paul Wilcox, USPACOM PR Analyst
   - SIPANET E-mail: paul.r.wilcox.ctr@pecom.scom.mil
   - NIPANET E-mail: paul.r.wilcox.ctr@pecom.mil
   - Phone: 808-477-7297
☐ Date SERE 100 Code of Conduct Level B Training completed?
☐ Date Personnel Recovery data validated?

PROTECTIVE MEASURES
☐ Protective measure attachments 1 and 2 provided to traveler(s)?

AT PLAN APPROVAL AUTHORITY
☐ AT Plan approved by appropriate authority?
   1. For countries that are at FPCON NORMAL or ALPHA - first O-5 in the traveler(s)/deployed unit’s chain of command.
   2. For countries that are at FPCON BRAVO, CHARLIE or DELTA - first O-6 in the traveler(s)/deployed unit’s chain of command.
   3. For travel to areas with a CDR USPACOM Travel Restriction, the first O-7 in the traveler(s)/deployed unit’s chain of command, must approve the AT Plan and certify that travel is deemed mission-essential.
LOSS PREVENTION PLAN

1. **Purpose.** To establish a Loss Prevention Plan to prevent loss of supplies, tools, equipment, or other materials in use, storage, or transit and during the issue process.

2. **Background.** The concern of the Department of the Navy is not only focused on the threat of criminal activity and acts of wrongdoing by forces external to the organizational unit, it is also specifically directed toward internal causes. Theft and pilferage by those who have authorized access, inattention to physical security practices and procedures, and disregard for property controls and accountability.

3. **Definitions**
   
   a. **Property.** Property consists of all assets. It includes all government and personal property, funds and negotiable instruments, tools and equipment, material and supplies, computer hardware and software, and information in the form of documents and other media. These assets are property whether categorized as routine or special, unclassified or classified, non-sensitive or sensitive, critical, valuable, or precious.
   
   b. **Pilferage.** Pilferage is petty larceny which means stealing of small items, generally of stored goods.
   
   c. **Theft.** Theft is a popular name for larceny. It is the taking of property without the owner’s consent, with intent to deprive the owner of the value of same, and to appropriate it to the use of benefit of the person taking.

4. **Responsibilities**
   
   a. Physical security of assigned COMNAVRESFORCOM spaces and equipment therein rests solely with the department/code inhabiting those spaces. All personnel should exercise individual responsibility for the care and protection of government property under his/her control/custody.
   
   b. All personnel are personally accountable for government-owned and assigned equipment. This accountability includes:
      
      (1) The proper use of such equipment.
      
      (2) Complying with the Command’s physical security regulations with respect to protection of equipment.
(3) Promptly reporting any missing, lost, stolen, or recovered equipment to the Physical Security Officer or their immediate supervisor

(4) Complying with established checkout procedures (i.e., accountability of all assigned property) when departing the Command.
## Pre Travel Training and Briefing Requirements

<table>
<thead>
<tr>
<th>Condition / Training Requirement</th>
<th>MILPERS Official Travel</th>
<th>MILPERS Personal Travel</th>
<th>CIVPERS Official Travel</th>
<th>CIVPERS Personal Travel</th>
<th>CIVILIAN FAMILY MEMBER Official Travel</th>
<th>CIVILIAN FAMILY MEMBER Personal Travel</th>
<th>CIVMARS Official Travel</th>
<th>CIVMARS Personal Travel</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOR Location Specific Brief (within 90 days of travel)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Level 1 ATEP Awareness Training (within 12 months of travel)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SERE: Level B Code of Conduct Training (within 24 months of travel)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>ISOPREP Validated in PRMS (1-Time input / updates as necessary)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IATP (approved at the required level)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Travel Clearance Request (if required) (submitted and approved within AF/ICS)</td>
<td>*Yes</td>
<td>*Yes</td>
<td>*Yes</td>
<td>No</td>
<td>*Yes</td>
<td>No</td>
<td>*Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Refer to DOD Foreign Clearance Guide for OCONUS travel: [https://www.fcg.pentagon.mil/](https://www.fcg.pentagon.mil/)