DEPARTMENT OF THE NAVY
PORTSMOUTH NAVAL SHIPYARD
PORTSMOUTH, NH 03804-5000

IN REPLY REFER TO:

NAVSHIPYD PTSMHINST 5510.25H
810
9 FEB 2021

NAVSHIPYD PTSMH INSTRUCTION 5510.25H

From: Commander, Portsmouth Naval Shipyard

Subj: ENTRY REGULATIONS FOR PORTSMOUTH NAVAL SHIPYARD

Ref: (a) DoD 5200.08-R, Physical Security Program
(b) DoD DTM 09-012, DOD Physical Access Control
(c) OPNAVINST 5530.14, Navy Physical Security and Law Enforcement Program
(d) NTTP 3-07.2.3, Law Enforcement and Physical Security
(e) CNICINST 5530.14E, Ashore Protection Program
(f) COMNAVREGMIDLANTINST 5530.14, Ashore Protection Program
(g) Real ID Act of 2005

Encl: (1) Official Function Access Request Template
(2) Private Function Access Request Template
(3) Official and Private Function Guest List
(4) Definitions
(5) Department of the Navy Local Population ID Card/Base Access Pass Registration

1. Purpose. Provide guidance and promulgate Portsmouth Naval Shipyard (PNS) access control policy as directed in references (a) through (g).

2. Cancellation. NAVSHIPYD PTSMHINST 5510.25G of 24 Oct 2017.

3. Effective Date. 11 February 2021

4. Policy. Access onto PNS will be either unescorted or escorted. This policy applies to personal or official visitors.

5. Scope

a. This policy applies to all military personnel, civilian employees, contractors, facilities, ships, tenant commands and non-Navy organizations physically located on or aligned to PNS.

b. All Tenant Commands, Unit Commanders, Officers-in-Charge, Facilities Managers, Department Heads and leaders must:

(1) Ensure their personnel understand and follow PNS access control policy and procedures.

(2) Develop internal access control procedures as directed in references (c) through (e) in protection of critical assets, restricted areas and other vulnerable areas.

6. Discussion

a. Successful installation access control is pivotal to the defense-in-depth concept and overall Force Protection (FP). It improves the probability of detection, and provides a strong psychological deterrent to potential aggressors who pose a threat to the installation.

b. The objective of installation perimeter access control is to physically control personnel and vehicular entry to installations, facilities, and resources.

(1) Authenticating an individual's identity and determining their fitness is a core principle of installation access control. The PNS' Commander (Code 100) will delegate PNS Pass and ID personnel to perform identity proofing, vetting, and determination of fitness. Personnel identified will be on a designated letter signed by Code 100.

(a) Identity proofing is the process of providing sufficient information (e.g., identity history, credentials, documents, etc.) when attempting to establish an identity.

(b) Vetting is an evaluation of an applicant's character and conduct for approval, or denial of the issuance of an access control credential for physical access.

(c) Fitness is the level of character and conduct determined necessary for the basis of access control decisions. For the purposes of this policy, fitness criteria are further defined as:

1. Person presenting the credential has been properly identity proofed and vetted.

2. Person has a credential authorized to facilitate access.

3. Person matches the credential authorized to facilitate access.

4. The individual must have a valid purpose to be on the installation and be properly sponsored, as applicable. Possession of an authorized and valid credential does not automatically authorize access to PNS. All persons requesting access must be checked against the barment list prior to getting a pass or entering the installation.

5. Authorized credential is still valid and not expired.

6. Person requesting access to PNS cannot have had a felony conviction within the last 10 years, including felony arrest not adjudicated or deferred. Any conviction of an offense meeting the sexual offender criteria. Any misdemeanor within the last five years, to include illegal possession and/or drugs, crimes of violence, sexual assault, larceny, and habitual offender. Additionally, a misdemeanor arrest not adjudicated or deferred. Any history of membership in any organization that advocates the overthrow of the U.S. Government. Barment from any Department of Defense (DoD) installation, which includes reciprocal barment from all installations.

7. Continuous evaluation provided via an identity management system (e.g., the Defense Biometric Identification System (DBIDS)) facilitates real time fitness determination.

(2) Access onto PNS will be either escorted or unescorted.

7. Procedure

a. Unescorted Access

(1) Unescorted access of DoD affiliated personnel

(a) Unescorted access is normally granted, after fitness for entry is conducted by an Entry Control Point (ECP) Sentry, to those personnel who present a credential authorized to facilitate access to an installation.

(b) Reference (f), section 1203, contains a comprehensive list of DoD authorized credentials facilitating access to an installation. The DOD Common Access Card (CAC) will be the principal card used to access buildings, facilities, installations, ships and controlled spaces.

(c) DoD affiliated personnel requesting unescorted access to PNS must be in physical possession of an authorized credential when permission is granted by ECP sentries. Personnel without an authorized credential shall not be granted access, even if the ECP sentry personally recognizes the person requesting access.

(2) Unescorted access of non-DoD affiliated personnel

(a) Non-DoD affiliated visitors must have a valid need to enter PNS and must be sponsored. Sponsors take full responsibility for verifying the need of the visit, and the conduct of their visitors while on the installation.

(b) In order to obtain unescorted access to the installation for their visitors, sponsors must comply with the following procedures:

1. Vetting and identity proofing of visitors requiring unescorted access can be accomplished with minimal delay (depending on the size of the group) at PNS Visitor Control Center (VCC) (Pass Office).

2. Sponsors must escort their visitor(s) to the VCC during normal working hours, where visitors 16 years and older must provide a fully completed SECNAV 5512/1 form, enclosure (1), this form is required to conduct the vetting process. The SECNAV 5512/1 form is the sole source to conduct background checks.

3. Visitors 18 years and older must present approved identification as part of vetting and identity proofing process. Reference (f), section 1204, provides a comprehensive list of approved identity proofing documents used to establish identity.

4. Vetting officials designated in writing will conduct background checks through Open Fox and Maine State utilizing Operator License Number and Social Security Number (SSN). Once cleared, Pass and ID will be notified by vetting official to process for access. If after hours vetting is needed, Dispatch will conduct vetting with same procedures, Watch Commander will be notified if the visitor is cleared or denied access. Visitors who successfully complete vetting and identity proofing will be issued a DBIDS credential. DBIDS credentials are normally issued for the duration of the visit, not to exceed 90 days. The visitor's credential/pass may be revoked for cause at any time, based on the actions of the individual or the sponsor.

b. Escorted Access

(1) Escort procedures may be used during Force Protection Condition (FPCON) NORMAL, ALPHA, and BRAVO, and as local security conditions permit, to facilitate access of non-DoD affiliated visitors, as well as DoD affiliated personnel who have misplaced their DoD credential, onto PNS. The DoD Trusted Traveler Program (TTP) allows escorted access of visitors without completing the vetting process required for unescorted access.

(2) Escort procedures allows an active duty military member or DoD civil service employee with a valid CAC, a military retiree with a valid DoD identification credential, or a military dependent of at least 16 years of age with a valid DoD identification credential, to present their identification for verification while vouching for and escorting non-DoD affiliated guests. The following is a list of categories of escorts and types of Identifications (ID) which may be used:

(a) Active Duty Military Members: CAC ID.

(b) Reserve Members: CAC ID.

(c) Military Dependents (age 16 or older): Military ID.

(d) Retired Military Members: Military ID.

(e) DoD Civil Service Employees - CAC ID.

NOTE: Contractors (even if issued a CAC), Volunteers or family care providers are not authorized to serve as escorts.

(3) Escort to visitor ratio

(a) The number of personnel an escort is allowed to escort is four. An escort must be inside the vehicle with the personnel they are escorting.

(b) If walking onto the installation, the escort to guest ratio shall not exceed four guests to one escort.

(4) Escorts, even for special events, must remain in the immediate presence of those being escorted at all times and are responsible for the actions of all personnel they escort. Escorts are reminded when escorting guests onto the installation, they must take special care to observe all applicable security procedures, to include controlled or restricted area limitations and maintaining Operational Security (OPSEC) practices.

(5) Escorted visitors may be asked by Navy Security Forces (NSF) at any time during a visit to present identification to establish identity.

c. Foreign Visitors. Foreign visitor access to PNS must be controlled properly to avoid inadvertent or unauthorized disclosure.

(1) Foreign Visitor – Official Visit

(a) Foreign visit requests are required for visits by official representatives of a foreign government or international organization to Department of the Navy (DoN) activities and cleared contractor facilities.

(b) Visit requests of official foreign military members, official foreign civilians and; in some circumstances their families, is accomplished in an official capacity through the DoD Foreign Visits System (FVS) and Foreign Visits System-Confirmation Module (FVS-CM) by the sponsoring person or organization. FVS and FVS-CM shall be used to verify the vetting of these personnel.

1. FVS-CM is the software application developed to track and confirm foreign visitors at all DoD component installations.

2. It is the sponsoring person/organization's responsibility to ensure official visits by foreign nationals is properly requested and approved in DoD FVS prior to entry onto PNS.

3. The sponsoring person or organization is responsible for notifying the Precinct Commander via the VCC of all approved requests of foreign military members, foreign civilians and their families.

(c) Official foreign national visitors who are not in possession of an issued DoD CAC shall be escorted at all times while on PNS by a member of the sponsoring command authorized to escort. Exceptions to this requirement must be approved by the Shipyard Commander, PNS.

(2) Foreign Visitor – Unofficial Visit

(a) Unofficial foreign national visits are visits by foreign nationals who are not representing their government in an official capacity (e.g., courtesy calls, public tours, students, etc.).

1. Unofficial visits are outside the scope of the FVS and instead shall be processed in accordance with DoD and DoN Personnel Security Program Directives.

2. Access to DoN and its cleared contractor facilities by such persons will be handled on the same basis as visits by U.S. citizens without security clearances.

(b) Escort requirements shall be adhered to for all unofficial foreign national visits aboard PNS.

(3) Naval Criminal Investigative Service (NCIS) notification of foreign visitor access.

(a) It is the sponsoring person or organization's responsibility to ensure the PNS NCIS Field Office is notified of both official and unofficial foreign national visits well in advance (5 to 10 business days) to facilitate additional vetting by NCIS.

(b) Furthermore, it is the sponsoring person or organization's responsibility to ensure the NCIS Field Office is notified when foreign visitors arrive and depart PNS.

d. Public Private Venture (PPV) Housing residents/DoD Affiliated Resident Guests

(1) PPV housing residents, located aboard and within the fence line of PNS, may sponsor non-DoD affiliated guests (i.e., personnel not in possession of a DoD authorized credential), escorting their guests or by applying for unescorted access for their guests.

(2) In order to obtain unescorted access to the installation for their guests, PPV housing residents must comply with the unescorted guest procedures stated above.

(a) Guests of residents who successfully complete identity proofing and vetting will be issued a DBIDS credential or pass.

(b) DBIDS credentials/passes are normally issued for the duration of the visit, not to exceed 30 days; however, may be issued for periods greater than 30 days. The visitor's pass may be revoked for cause at any time, based on the actions of the individual or the sponsor.

e. Special Credentials Facilitating Access. There are numerous authorized credentials that facilitate access to an installation. Reference (f), section 1203 provides an extensive list of DoD authorized credentials. The following amplifying guidance is provided:

(1) Transportation Worker Identification Credential (TWIC)

(a) Administered by the Transportation Security Administration (TSA) and U.S. Coast Guard, personnel in possession of a valid TWIC are considered identity proofed for the purpose of installation access. However, these individuals are not allowed access without additional vetting, fitness determination, sponsorship, and a valid bill of lading/work order.

(b) TWIC holders must meet the following conditions prior to being allowed unescorted access:

1. Possess a valid TWIC which shall be electronically validated using a DBIDS scanner.

2. Demonstrate a valid purpose for entry by presenting a work order, bill of lading, etc.

(c) In addition to electronically validating the TWIC using a DBIDS scanner, prior to granting access, ECP sentries shall conduct a second vetting of the individual's background via VCC.

(2) DBIDS Credential and Paper Access Pass

(a) DBIDS credentials and paper access passes are locally generated at PNS' VCC following successful vetting and identity proofing.

(b) DBIDS credentials and paper access passes are normally issued for the duration of visit and will provide access only at the base issued. Therefore, a DBIDS credential or paper access pass issued from an installation other than PNS shall not be honored.

(c) Eligible Populations. Populations requiring intermittent or routine installation access may include, but are not limited to, contractors, employees, volunteers, visitors (official and unofficial), transportation organizations (taxi, share ride, bus/transit companies), service providers (bank/credit unions), vendors, interns, DoD civilian retirees, and privatized housing occupants, Special Agents, Agent and Assist personnel, and Gold Star Family Members.

(d) DBIDS credentials will be issued for periods longer than 90 days (credential only). Paper DBIDS access passes may not be issued for a period longer than 90 days. Personnel will be vetted every 90 days.

(e) Like TWIC credentials, all DBIDS credentials and paper access passes shall be electronically validated using a DBIDS scanner prior to granting access.

(3) Department of Homeland Security Real Identification Act of 2005 Compliance

(a) The Real ID Act was designed to help standardize access across federal agencies. Many States are either in compliance with standards, or showing progress toward meeting standards and thereby granted waivers allowing those state identifications to be used for the purpose of identity proofing.

(b) Individuals who provide a state driver's license from these states (that do not meet the Real ID Act requirements) must provide an additional form of identification listed in section 1204 of reference (f), which provides a list of approved identity proofing documents used to establish identity.

NOTE: Individual command (e.g. Naval Sea Systems Command (NAVSEA) Badge) and activity supplemental badges are not authorized credentials facilitating access to an installation. These badges are not acceptable for granting access to PNS.

(c) Single Source Coordinator (SSC) Program

1. The PNS Navy Exchange serves as the PNS SSC. The SSC shall manage and administer the program per references (f) and (g).

2. Transportation services, to include but not limited to taxicab, limousine, ride share (e.g., UBER, LYFT, etc.), and shuttle services, desiring access onto PNS, shall register with the SSC. Ride share drivers (e.g., UBER, LYFT) with an authorized DoD credential that authorizes escort privileges may be granted access aboard the installation.

3. Once registered, the VCC shall ensure proper vetting, ID, and verify proper registration. VCC will issue a DBIDS credential to facilitate access onto PNS.

4. All transportation vehicles will be inspected and all personnel requiring access to PNS will have a valid form of ID to enter PNS.

5. Transportation service companies are prohibited from entering restricted areas and are limited to movement to and from the fare pickup and drop-off destination.

6. Services shall normally be restricted in FPCONs CHARLIE and DELTA.

(d) Media. Any request for entry by civilian news, radio, television, or other media shall be referred to the Public Affairs Officer prior to allowing access to the installation, and

shall be escorted at all times. Escorts will be provided by the host command, and the TTP escort policy and procedures apply.

(e) Emergency Vehicles (EV) Access

1. Federal/State/Local Law Enforcement Officers in marked and/or official unmarked vehicles will be allowed entry and/or departure through any gate when conducting business on PNS.

2. Other First Responders (e.g., Fire, Medical, etc.) in EVs will be allowed entry and/or departure through any gate when conducting business on PNS.

a. In order to prevent loss of life, these agencies shall be passed onto the installation unimpeded when in response to a "true emergency."

b. ECP Sentries will immediately notify their Watch Commander (WC) whenever a First Responder is allowed to enter under "true emergency" circumstances.

3. EVs arriving at an ECP unannounced not in emergency mode (e.g., lights and/or sirens) will be vetted and ID proofed by ECP sentries.

a. The ECP sentry will conduct a visual check of the driver's official credential, the interior of the vehicle, verify none of the occupants are under duress and be alert for anything unusual prior to granting access.

b. The ECP sentry will pass to WC the agency name, unit number and destination via radio.

(f). Special Events. Deploying and Returning Afloat Units:

1. Access to PNS by non-DoD affiliated guests of deploying or returning afloat unit personnel will be facilitated either by escort or unescorted privileges after vetting as described in subparagraph 6a (2) of this instruction.

2. The deploying or returning unit must provide a fully completed and alphabetized list to NSF Physical Security (Code 810) for vetting no fewer than 30 days prior to the scheduled return/departure date.

3. Guests shall be directed to arrive at a specified gate as coordinated with NSF, present an authorized identification (reference (f), section 1204, provide a comprehensive list of approved identity proofing documents used to establish identity), be confirmed they are on the guest list, and then be granted access to the installation.

4. Guests are the responsibility of the sponsor. The sponsor will ensure:

a. POCs are available at each designated ECP to de-conflict any issues that may arise.

b. Guests are provided directions to and from the event location, and instructed not to deviate away from the specified route. The sponsor shall place directional signs along the specified route.

c. Guests are advised of firearms and photography restrictions, as well as remaining clear of restricted areas (e.g., munitions area, etc.).

(4) Large Scale Special Events

(a) Events onboard PNS where escort and vetting of non-DoD affiliated guests is not practical (e.g., a ship commissioning) shall be approved via the Special Event Antiterrorism (SEAT) planning process per references (e) and (g).

(b) The event sponsor shall develop and submit the SEAT in coordination with NSF, for approval by the appropriate Echelons of command, including Commanders who have Tactical Control (TACON) for FP, no later than 30 days prior to the event per references (e) and (g).

j. Vehicle Inspections – Installation and Restricted Areas

(1) Inspection of vehicles, including but not limited to personal operated vehicles, commercial delivery vehicles, contractor vehicles, and Government or Government leased vehicles, entering PNS shall align with requirements of the current FPCON and the Random Antiterrorism Measure (RAM) schedule.

(2) In accordance with references (c) through (e), all vehicles entering restricted areas within PNS, shall undergo a complex vehicle inspection.

(a) A complex vehicle inspection is defined in reference (d).

(b) The complex vehicle inspection shall be conducted by the Vehicle Inspectors at George 1 Commercial Vehicle Inspection Station (CVIS) prior to granting access to Paul 2.

(3) Installation access for commercial delivery or contractor vehicles of companies enrolled in the DBIDS program whose drivers have been issued a DBIDS credential will not normally be subjected to vehicle inspections at PNS CVIS. Additionally, delivery vehicles driven by Government Service employees issued a CAC will not be subjected to vehicle inspections at PNS CVIS.

(a) These vehicles will be allowed to bypass PNS CVIS and will only be inspected in conjunction with PNS RAM program, or prior to being granted access to a pier where naval vessels are berthed, or other restricted areas.

(b) PNS will continue to inspect all commercial delivery and contractor vehicles whose drivers are not enrolled in DBIDS or issued a CAC at PNS CVIS in an effort to mitigate the risk of transportation of contraband and Chemical, Biological, Radiological, Nuclear, and high-yield Explosive (CBRNE) aboard the installation.

(4) All non-DBIDS and non-CAC vehicles inspected at PNS CVIS, and DBIDS and CAC vehicles randomly selected for inspection during RAMs, will receive a vehicle pass indicating the vehicle was inspected, with a date and time of inspection. This pass will be maintained by the driver upon entering the installation.

(5) To ensure compliance with references (c) through (e) directive to inspect all vehicles entering a restricted area, including a pier, with a complex vehicle inspection, all pier ECP sentries under the TACON for FP of PNS will ensure the following:

(a) For all non-DBIDS and non-CAC credentialed commercial delivery and contractor vehicles:

1. Conduct an identity check by verifying the validity of the driver's credential.

2. Establish the driver's need to enter the restricted area (e.g. pier) by verifying the delivery bill of lading and/or work order, and confirm delivery with the destination command's quarterdeck.

3. Verify all non-DBIDS and non-CAC commercial delivery and contractor vehicles entering the restricted area (e.g. pier). Ensure ECPs have received a complex vehicle inspection at PNS CVIS and are in receipt of a valid PNS vehicle access pass with the current date and time of inspection indicated.

4. If the vehicle pass is valid (arrived at the ECP following inspection within the specified time indicated on the pass), permit access to the restricted area without conducting an additional complex inspection.

5. If the driver is not in possession of a valid pass, or if the pass is not valid (did not arrive at the restricted area ECP following inspection within the specified time indicated on the pass), conduct a complex vehicle inspection by the ECP Vehicle Inspection Team (VIT) at the restricted ECP.

(b) For all DBIDS and CAC credentialed delivery vehicles:

1. Conduct an identity check by verifying the validity of the driver's credential.

2. Establish the driver's need to enter the restricted area (e.g. pier) by verifying the delivery bill of lading and/or work order, and confirm delivery with the destination command's quarterdeck.

3. If the vehicle pass is valid (arrived at the ECP following inspection within the specified time indicated on the pass), permit access to the restricted area without conducting an additional complex inspection.

4. If the pass is not valid (did not arrive at the ECP following inspection within the specified time indicated on the pass), conduct a complex vehicle inspection by the ECP VIT at the restricted area ECP.

(6) Inspection of Government Owned Vehicles (GOV) and EV.

(a) In accordance with reference (e), the Shipyard Commander is authorizing the exemption from complex vehicle inspections of those GOVs, including Government leased vehicles, requiring frequent pier access. Specifically, Naval Facilities Engineering Command (NAVFAC), Port Operations, and PNS NSF vehicles are exempt.

(b) Exemption from complex vehicle inspections at pier ECPs shall be subject to the following requirements:

1. A list of exempted GOVs, to include identifying vehicle information, must be provided to NSF.

2. Exempted GOVs must be inspected at regular intervals, not to exceed 30 days.

3. Complex vehicle inspection of these GOVs will be conducted at PNS CVIS, upon which a 30-day GOV vehicle inspection pass embossed with the PNS seal will be issued depicting the date of inspection and inspection expiration date.

4. If the GOV is taken outside the confines of PNS, the vehicle must be re-inspected at PNS CVIS and issued a new 30-day vehicle inspection pass.

(c) All pier ECP sentries TACON to PNS for FP shall ensure the following for all government licensed and leased GOVs entering pier ECPs:

1. Conduct an identity check by verifying the validity of the driver's credential.

2. Establish the driver's need to enter the pier by verifying delivery bill of lading and/or work order, if applicable.

3. Verify all GOVs entering pier ECPs have received a complex vehicle inspection at PNS CVIS and are in possession of a valid 30-day vehicle inspection pass embossed with the PNS seal.

4. If the vehicle pass is valid, permit access to pier without conducting an additional complex inspection.

5. If the driver is not in possession of a valid pass, or if the pass is expired, conduct a complex vehicle inspection at ECP 1 or 2.

(d) NAVFAC, Port operations, and NSF vehicles in possession of a valid 30-day vehicle inspection pass embossed with the PNS seal shall be afforded head of the line privileges to facilitate effective and efficient operations on the waterfront.

(e) Vehicle inspections at the pier ECP shall be conducted in an area that does not impede the flow of vehicle traffic on and off the pier.

(f) Non-NSF Emergency Vehicles. Non-NSF emergency vehicles (fire and ambulance) in the non-emergency mode shall be granted access to piers following verification of driver's access credential and completion of a complex vehicle inspection, unless the emergency vehicle is responding to the pier in emergency mode (e.g., activated emergency lights or activated emergency lights and sirens) or in possession of a valid 30-day vehicle inspection pass embossed with the PNS seal.

k. Access Control ECP Operations

(1) Structure of an ECP

(a) An ECP is subdivided into zones, each encompassing specific functions and operations. Beginning at the installation property boundary, the zones include the Approach Zone, Access Control Zone, and Response Zone. Situational awareness must be focused on vehicles and pedestrians approaching the ECP and enter each zone:

1. The Approach Zone lies between the installation boundary and the access control zone. It is the interface between the off-installation road network, the installation and the area all vehicles must traverse before reaching the actual checkpoint. The approach zone must support the following functions and operations:

a. Traffic calming/slowing

b. Traffic sorting and stacking

c. Provide the first opportunity to identify potential threat vehicles, including those attempting entry through the outbound lanes of traffic.

2. The Access Control Zone is the main body of the ECP and includes guard facilities and traffic management equipment. Access determination for entry is performed by the contact sentry in this zone.

3. The Response Zone is the area extending from the end of the access control zone to the final denial barrier. This zone defines the end of the ECP. The response zone should be designed so sentries have time to react to a threat, operate the final denial barriers, and close the ECP if necessary.

(b) Installation jurisdictional boundaries beyond or outside ECPs are delineated by blue painted lines marked U.S. Government Property.

1. These lines delineate where Government property begins/ends, and is intended to clearly identify, as a visual representation and notification, to personnel approaching the installation ECP they are entering U.S. Government property.

2. These lines also provide the NSF a clear visual representation of U.S. Government property for purposes of jurisdiction and authority when responding to incidents in and around ECPs. Response to incidents outside these blue lines shall be by applicable city, state, and federal civilian authorities.

(c) ECP contact sentries shall decisively control vehicle and pedestrian traffic entering each ECP zone through effective verbal and non-verbal communications to achieve safety and NSF while precluding breeches of perimeter/unauthorized entries. To that effort, contact sentries shall:

1. Establish and maintain eye contact with the driver of each vehicle approaching and transiting through the access control zone.

2. Direct the driver to stop at the lane stop sign/stop line/"proceed when directed by sentry" sign using non-verbal communications. Specifically, the sentry will hold out his/her non-firing arm straight out in front, palm facing the vehicle as it approaches, indicating the vehicle must stop.

3. Conduct an assessment of the vehicle and occupants, and when ready, provide the driver non-verbal direction to proceed forward by bringing his/her lower arm straight across the chest in a sweeping movement in a professional manner. Multiple sweeping movements is not normally required if effective eye contact with the driver is maintained.

4. As the vehicle proceeds forward, the contact sentry shall hold out his/her left arm straight out at a right angle to their side, palm facing the vehicle as it approaches, indicating where the vehicle must stop.

5. Once the vehicle has come to a complete stop, the contact sentry will begin the access determination process.

(2) Credentials shall be physically handled by the contact sentry, and must be removed from any container, holder, protector, etc., during the access determination process. Do not accept or scan identifications in any container, holder, protector, etc.

(3) DBIDS Scanners

(a) Use of DBIDS scanners is mandatory at all times to conduct access determination of vehicle occupant(s) and pedestrians prior to granting access to the installation.

1. The goal is DBIDS scanning of every pedestrian and vehicle entering PNS with exceptions stated below and in references (f) and (g).

2. DoD authorized credentials facilitate access to an installation without a barcode will be physically and visually validated (e.g., face to picture match, current expiration date/not expired), condition inspected (e.g., signs of tampering), and individual allowed entry accordingly. Reference (f), section 1203, contains a comprehensive list of DoD authorized credentials facilitate access to an installation.

(b) In FPCON BRAVO and below, only single scan (e.g, DBIDS scanning of credential) and identity proofing (e.g., face to picture match, current expiration date/not expired, signs of tampering) is required. All occupants of a vehicle are required to present an identification to gain access.

1. At least one person in the vehicle must be in possession of a DoD authorized credential facilitating access to an installation.

a. Others not in possession of an authorized credential may be escorted under the DoD TTP as described above.

b. This authorization is restricted as the FPCON increases.

2. Contractors even if issued a CAC, are not allowed to act as Escorts. If a credentialed contractor driving a vehicle provides a CAC or DBIDS credential, access determination is required for all occupants for proper credentials before allowing entry regardless of how many personnel are in a vehicle.

(c) Exceptions to use of DBIDS Scanners

1. Watch Commanders or section leadership may authorize "flash pass" during high peak times (e.g., morning rush hour) and only if traffic is congested.

a. The determination of congested requires the NSF (e.g., most senior or experienced) at the ECP to use their discretion and judgment.

b. Authorization WILL be obtained from the Watch Commander, Assistant Watch Commander or Section Lieutenant (LT) before executing "flash pass", and even when authorized a random number of credentials must be scanned using DBIDS scanners; number determined by the Watch Commander, Assistant Watch Commander, or LT (e.g, every 10th vehicle).

2. "Flash Pass" is defined as access determination via a physical and visual validation of the credential to the owner (e.g., face to picture match, current expiration date/not expired) and inspection of the condition of the card (e.g., signs of tampering).

3. "Flash Pass" does NOT apply to the DBIDS credential, paper pass, or TWIC credentials.

a. 100 percent DBIDS scanning is mandatory of these credentials unless the scanners are inoperable at the ECP. If inoperable, a physical and visual verification is acceptable until the scanners are operating.

b. If the scanners cannot be repaired for an extended period of time, the person shall be directed to a gate where the scanners are operating for proper vetting.

(d) DBIDS Scanning Access Recommendations: Upon scanning the barcode of a credential, the Access Recommendation Screen appears showing the picture and biographic information associated with the scanned credential. Background color of the screen indicates access recommendation:

1. Green: Indicates the cardholder is authorized entry. Sentry should select the desired button (e.g., Grant Access) with the stylus or finger, allow access after vetting, identity proofing, and fitness for entry process is complete.

2. Yellow: A warning indicates a problem or alert merits investigation but does not automatically prohibit the cardholder from access. Sentry should choose "Tap for more" underneath the access recommendation (e.g., top-right portion of the screen), review additional information and if necessary request additional vetting information from the VCC or Watch Commander. Contact section leadership for guidance prior to granting access. Upon access decision, select the desired button (e.g., Grant Access or Deny Access) with the stylus or finger.

3. Red: Indicates the cardholder is not authorized entry to the base. Sentry should choose "Tap for more" underneath the access recommendation (top-right portion of the screen), review additional information and if necessary request additional vetting information from the VCC or Watch Commander. Contact section leadership for guidance prior to granting access. DO NOT ALLOW ACCESS UNTIL CLEARED BY NSF SECTION LEADERSHIP if a red Person Status displays (e.g. armed and dangerous, barred, call law enforcement, etc.). Upon access decision, select the desired button (e.g., Grant Access or Deny Access) with the stylus or finger.

(e) Personnel with Wants/Warrants shall be processed as follows:

1. Military

a. Verify want/warrant with DC.

b. Detain member if confirmed. Release on own recognizance if not confirmed.

c. Contact issuing agency to determine extradition.

d. If extraditable and agency will come pick the person up, contact the service member's Command Duty Officer (CDO) for them to coordinate with their Commanding Officer (CO) to arrange the release of the military member to the issuing agency. The military member's CO must authorize the release of the military member prior to the release. Do not release unless approved by the member's CO.

e. If not extraditable or agency will not come pick up, release to the military member's CDO.

f. Do not confiscate military CACs or issue a debarment letter.

2. Civil Service Employee

a. Verify want/warrant with Dispatch Center.

b. Detain member if confirmed. Release on own recognizance if not confirmed.

c. Contact issuing agency to determine extradition.

d. If extraditable and agency will come pick the person up, release to agency.

e. If not extraditable or agency will not come pick up, confiscate CAC, issue receipt and place in case report file, issue temporary debarment letter, escort to nearest ECP and release.

3. Contractors/Other

a. Verify want/warrant with Dispatch Center.

b. Detain member if confirmed. Release on own recognizance if not confirmed.

c. Contact issuing agency to determine extradition.

d. If extraditable and agency will come pick the person up, release to agency.

e. If not extraditable or agency will not come pick up, confiscate CAC/DBIDS issue receipt and place in case report file, issue temporary debarment letter, escort to nearest ECP and release.

(4) Traffic Controlling and Calming Measures

(a) NSF Patrol Section leadership is expected to utilize Use of Hardened Access Control System (HACS) barriers at ECPs during off-peak traffic periods. Crash beams are lowered at George-2 when gate is secured.

(b) Example (A): Crash beams lowered in inbound Lanes 1 and 2, and in the up position of inbound Lane 3, but red and white traffic arms lowered in Lanes 2 and 3 requiring the vehicle to serpentine over to Lane 1 for access determination. For outbound lanes, lower crash beams in outbound Lanes 4 and 5 allowing exit only from Lane 6. This would cause someone trying to enter in the outbound lanes to sharply maneuver over to the left to enter, thereby assisting in delaying entry while helping determine intent of the driver.

(5) Personnel ID Management

(a) Lost Identifications. All lost IDs must be reported immediately to NSF or the Base Support Office.

(b) Termination of Employment. All IDs shall be relinquished to the employing agent upon termination of employment.

(c) Confiscating Unauthorized Identification

1. NSF will confiscate any pass or identification card in possession of anyone other than the person to whom it was issued, or rendered invalid by reason of expiration, tampering, or modification.

2. Upon confiscating the pass or identification card, the confiscating authority will issue the individual a "Receipt for Military/Government I.D. Card." The original receipt will be provided to the individual, and a copy will be submitted to the Watch Commander for proper processing with the confiscated ID attached.

8. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per SECNAV M-5210.1 of September 2019.

9. Review and Effective Date. Per Office of the Chief of Naval Operations (OPNAV) Instruction OPNAVINST 5215.17A, the Executive Support Office (Code 1100) will review this instruction annually on or before the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, SECNAV, and Navy policy and statutory authority. This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV M-5215.1 of May 2016.

10. Forms. SECNAV Form 5512/1 which is listed as enclosure (5), can be found with this hyperlink:
https://www.cnic.navy.mil/content/dam/cnic/cnrsw/NBVC/pdfs/SECNAV5512%20%20Highlighted%20WITH%20EDIPI.pdf

D. W. ETTLICH

Releasability and distribution:
This instruction is not cleared for public release and is available electronically only via the PNS Instructions and Notices Web site.
A, O, 1104.1

OFFICIAL FUNCTION ACCESS REQUEST TEMPLATE

5530
Ser xxx/xx
XX XXX XX

From: Commander, NAME OF COMMAND
To: Commander, Portsmouth Naval Shipyard

Subj: OFFICIAL FUNCTION INSTALLATION ACCESS REQUEST

Encl: (1) Official Function Guest List

1. Commander, COMMAND NAME will host an invitation only official function onboard Portsmouth Naval Shipyard (PNS) on DAY, MONTH, YEAR from 1700 until 2200. Request the guests listed in enclosure (1) be granted access to PNS via Gate NUMBER, to attend this COMMAND hosted event at LOCATION (e.g., residence or chapel). As previously coordinated, guests will arrive with proper identification.

2. My point of contact for this event is LT JOHN DOE, at (207) XXX-XXXX or email at xxxx@navy.mil.

F. M. LAST

PRIVATE FUNCTION ACCESS REQUEST TEMPLATE

5530
Date

From: Commander, NAME OF COMMAND
To: Commander, Portsmouth Naval Shipyard

Subj: PRIVATE FUNCTION INSTALLATION ACCESS REQUEST

Encl: (1) Private Function Guest List

1. I will host an invitation only private function onboard Portsmouth Naval Shipyard (PNS) on DAY, MONTH, YEAR from 1700 until 2200. Request the guests listed in enclosure (1) be granted access to PNS via Gate NUMBER, to attend this COMMAND hosted event at LOCATION (e.g., residence or chapel). As previously coordinated, guests will arrive with proper identification.

2. My point of contact for this event is LT JOHN DOE, at (207) XXX-XXXX or email at xxxx@navy.mil.

F. M. LAST

OFFICIAL AND PRIVATE FUNCTION GUEST LIST

Date of Event	Time From	Time To	Non-DoD Guest Last Name	First Name	Event	Sponsor	POC	POC Number

DEFINITIONS

1. Escorted Individuals. Personnel who require access, without determination of fitness, must be accompanied by a sponsor with authorization to escort. The sponsor accepts responsibility for the fitness and conduct of the escorted person and the escort requirement is mandated for the duration of the person's visit.

2. Unescorted Individuals. Personnel who have been favorably vetted, identity proofed, and issued an authorized access credential or pass. However, they are still subject to any controlled or restricted area limitations, as appropriate.

a. Terms associated with access control, and escorted and unescorted individuals:

(1) Access Determination. Action(s) taken by a sentry to determine the validity of an individual's authorization to access the installation or restricted area. Actions include, but are not limited to, electronic scan of access credentials, visual verification of credentials, review of access lists, etc.

(2) Commercial Vehicles. Vehicles owned by commercial agencies, operated by contractors, and licensed as a commercial vehicle.

(3) Contractors. Vendors, suppliers, and service providers licensed to conduct business by a State, who requires access to the installation to provide goods or services.

(4) Escort. An active duty military member or Department of Defense (DoD) civil service employee with a valid Common Access Card (CAC), a military retiree with a valid DoD identification credential, or a military dependent of at least 16 years of age with a valid DoD identification credential, to present their identification for verification while vouching for and escorting non-DoD affiliated visitors. Contractors, even if issued a CAC, volunteers or family care providers are not authorized to serve as escorts.

(5) Foreign Visitors (Unofficial). Foreign nationals who are not representing their government in an official capacity; for example, courtesy calls, public tours, students, etc.

(6) Immediate Presence. When escorting, immediate presence means within direct visual contact. When escorting a visitor in a vehicle, immediate presence is within the same vehicle.

(7) Sponsor. Active Duty, Guard and Reserve personnel on official orders, CAC holders (to include Contractor CAC holders), and family members 16 years of age and older are authorized to sponsor non-DoD affiliated guests onto an installation by applying for unescorted access for their guest(s). Sponsor authorization is different than escort authorization.

(8) Sponsorship. Sponsorship allows authorized sponsors to take responsibility for verifying and authorizing an applicant's need for access to an installation.

(9) Trusted Traveler Program (TTP). A DoD Program allowing an active duty military member or DoD civil service employee with a valid CAC, a military retiree with a valid DoD identification credential, or a military dependent of at least 16 years of age with a valid DoD identification credential, to present their identification for verification while vouching for and escorting non-DoD affiliated guests.