DEPARTMENT OF THE NAVY

NAVAL STATION NEWPORT
690 PEARY STREET
NEWPORT, RI 02841-1522

IN REPLY REFER TO:

NSNPTINST 5530.6C
N3AT
MAY 2 2 2018

NAVSTA STATION NEWPORT INSTRUCTION 5530.6C

From: Commanding Officer, Naval Station Newport

Subj: NAVAL STATION NEWPORT INSTALLATION ACCESS CONTROL

Ref: (a) DoD DTM 09-012, Interim Policy Guidance for DoD Physical Access Control
(b) DoDI 1000.13, Identification Cards for Members of the Uniformed Services
(c) DoDI 2000.16, DoD Antiterrorism (AT) Program Implementation
(d) SECNAV M-5210.1
(e) OPNAVINST 5530.14E, CH-3
(f) CNICINST 5530.14A, CH-2
(g) OPNAVINST 1752.3
(h) BUPERSINST 1750.10
(i) DoD 5200.08-R, Physical Security Program
(j) DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board
(k) DoD AT Guide
(l) COMUSFLTFORCOM OPORD 3300-15
(m) USNORTHCOM INSTRUCTION 10-222
(n) SECNAV memo of 7 Oct 08
(o) SECNAV M-2510.1
(p) CNIC N3AT HPD Advisory #09082014063 of 16 Sep 14
(q) COMNAVREGMIDLANTINST 5530.14A
(r) NAVSTANPTINST 5100.1G

Encl: (1) APPENDIX 2 TO ANNEX M TO AT OPORD 3300 ACCESS CONTROL

1. Purpose. This instruction establishes Commanding Officer (CO), Naval Station Newport (NSNPT) access control policy and minimum security standards for controlling entry to NSNPT and stand-alone facilities (hereafter referred to as installations). This instruction is per access control policies set forth in references (a) through (r).

2. Cancellation. NAVSTANPTINST 5530.6B.

3. Scope and Applicability. This instruction applies to all NSNPT and Tenant Command personnel.

4. Background

a. Responsibility. Per references (j) through (l), the NSNPT CO will establish, implement, and sustain scalable Base Operating Support (BOS) related access control procedures (ACP). These procedures are based on guidance from Commander, U.S. Fleet Forces Command; Commander, Navy Installations Command (CNIC); Commander, Navy Region Mid-Atlantic (CNRMA); Required Operational Capability (ROC) Levels; and Force Protection Conditions (FPCON). Implementation of this instruction meets or exceeds established personnel and access control guidelines.

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

5. Policy. Per references (a) through (r), the primary objectives of the NSNPT ACP are:

a. Consolidation of Higher Headquarters policy and guidance pertaining to access control into a single instruction.

b. Protect personnel and critical operational assets on board NSNPT and associated Tenant Commands.

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

d. Establish the following minimum access standards for all unescorted individuals, who must:

(1) Have a valid purpose to enter the installation

(2) Be identity-proofed

(3) Be identity-vetted

(4) Possess a valid installation access credential

e. Establish and validate requesting personnel's background utilizing the following methods:

(1) The National Crime Information Center (NCIC) Database

(2) The Terrorist Screening Database

(3) The Sex Offender Registry & Notification Act (SORNA)

(4) The Consolidated Law Enforcement Operations Center (CLEOC)

(5) The Foreign Visitor System – Confirmation Module (FVS-CM)

(6) The Department of Homeland Security (E-Verify)

(7) The Department of Homeland Security (U.S. VISIT) and

(8) The Department of State Consular Checks (non-U.S. citizen)

f. Personally Identifiable Information (PII) collected and utilized in execution must be safeguarded to prevent any unauthorized use, disclosure, and or loss, per reference (o).

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

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

b. The following personnel are authorized unescorted access and need no further vetting. Additionally, these personnel can serve as Escort/Trusted Traveler/Sponsor for installation access during Force Protection Conditions (FPCON) Normal, Alpha, Bravo, and as detailed in enclosure (1).

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

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

(1) Department of Defense (DoD) Military Personnel are vetted with a National Agency Check for Law and Credit and, when in possession of a CAC ID, have met the requirements of paragraph 5.

(2) A DoD Civilian Personnel National Agency Check with Inquiries (NACI) and, when in possession of a CAC ID, have met the requirements of paragraphs 6.a and 6.b.

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

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

d. Military and DoD civilian retirees are not authorized to serve as sponsor.

e. Contractors are not authorized to serve as trusted traveler escort or sponsor.

7. Gold Star Family Members.

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

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

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

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

e. Gold/Blue star personnel requesting access to NSNPT will be granted access after successfully meeting the requirements in paragraph 5.

8. Additional Considerations

a. Local installation access credentials are developed, issued, and tracked using the Defense Biometric Identification System (DBIDS). DBIDS is a Physical Access Control System (PACS) developed by the Defense Manpower Data Center (DMDC) which uses existing DoD records and information, digital images, and digital fingerprints to facilitate issuing credentials to

individuals who are otherwise not authorized a DoD credential. The system is configured to DoD, U.S. Navy, and NSNPT unique requirements. Enclosure (1) outlines requirements for obtaining DBIDS credentials for vendors. Vetting request will be coordinated through the Pass and ID office: W_NWPT_GPASS_ID_GS01@NAVY.MIL, Phone: (401)841-3126, DSN: 841-3126, open 0700-1530 Monday – Friday.

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

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

d. Enclosure (2) of reference (q) provides relief from these access control requirements (and specific direction) for support of senior officer events occurring on installation.

9. Records Management. Records created as a result of this instruction, regardless of media and format, will be managed per reference (o). Particular attention shall be given to ensure all PII is strictly guarded, which includes proper encryption if transmitted via email. If PII information cannot be encrypted, it must be hand delivered, not emailed.

10. Review and effective date. Per OPNAVINST 5215.17A, the Security Director will review this instruction annually on the anniversary of its 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.

I. L. JOHNSON

Releasability:
This instruction is cleared for public release and is available electronically only via Gateway 2.0 Website, https://g2.cnic.navy.mil/Directives/Documents/Forms/RegionInstallation.aspx?FilterField1=Region0&FilterValue1=CNRMA&FilterField2=Installation0&FilterValue2=NAVSTANEWPORTRI

APPENDIX 2 TO ANNEX M TO AT OPORD 3300

ACCESS CONTROL

1. Mission. See Base Plan.

2. Situation. Provide guidance to establish and prescribe procedures for access control at Naval Station Newport (NSNPT). This instruction does not address internal movement controls. These capabilities are dynamic and will be reviewed on a regular basis. Specific program items include:

a. Verification of personnel and vehicle access, identification, and movement control as a means to identify and account for personnel and vehicles authorized access to NSNPT. The commanding officer (CO) has the authority to alter and enforce additional access control policy measures during elevated Force Protection Conditions and emergent situations to protect persons and property on the installation.

b. The NSNPT installation access control plan addresses the following:

(1) Installation access locations

(2) Types of installation access

(3) Installation access credentials

(4) Local installation access credentials

(5) Vetting processes and procedures

(6) Other installation access control considerations, e.g. lost, stolen, or forgotten installation access credentials; access control at each Force Protection Condition (FPCON); Mission Essential Personnel (MEP); emergency responder access; etc.

3. Execution

a. Installation access locations

(1) Vehicle Entry Control Points (ECP).

(a) Gate 1 – Normally open continuously.

(b) Gate 2 – Normally open Monday-Friday, 0630-0830.

(c) Gate 17 – Normally open Monday-Friday, 0600-1800.

(d) Gate 7 (Naval Health Clinic New England (NHCNE)) – Normally open Monday-Friday, 0700-1900; Saturday, 0700-1300.

(e) Gate 23 (Naval Undersea Warfare Center (NUWC)) –Normally open continuously.

(f) Gate 32 (NUWC) – Normally open Monday-Friday, 0615-0900 and 1530-1730.

(g) Pedestrian access allowed at all vehicle ECPs during normal operating hours.

(2) Pedestrian ECPs

(a) Gate 11 pedestrian turnstile –open 24/7, automated entry control via Lenel programmed magnetic strip on Common Access Cards (CAC). Operates on magnetic card swipe only –no pin required.

(b) Gate 23 Pedestrian turnstile - open 24/7, automated entry control via Lenel programmed magnetic strip on Common Access Cards (CAC). Operates on magnetic card swipe only –no pin required.

b. Types of installation access

(1) Unescorted – individuals who have been identity proofed, favorably vetted, issued an access credential, and are authorized to be on an installation without an authorized sponsor or escort being present. These individuals are still subject to any controlled or restricted area limitations, as appropriate.

(2) Escorted – individuals who do not have an access credential and require access without a determination of fitness. They must be accompanied by an eligible escort.

(a) Trusted Traveler. Trusted Traveler procedures allow the following individuals, to present their ID card for verification while simultaneously vouching for individuals accompanying them.

1. A uniformed service member with a valid CAC.

2. A DoD employee with a valid CAC.

3. A retired uniformed service member with a valid DoD credential.

4. A dependent, 16 years of age and older, with a valid DoD credential.

(b) The following provisions apply to trusted traveler escorts.

1. The maximum number of individuals a trusted traveler escort can vouch for is eight.

2. A trusted traveler escort must remain in the immediate vicinity of the individual(s) being escorted.

3. A trusted travel escort assumes full responsibility for the conduct of escorted individual(s).

4. A trusted traveler escort cannot vouch for an individual(s) in a separate vehicle, except in a situation where it is unfeasible to accomplish same vehicle escort, e.g. escorting a crane and operator onto the installation. Upon arrival at the destination all other trusted traveler provisions remain applicable. This will only be considered if vetting and pass issuance cannot be accomplished.

5. Contractors, volunteers and family care providers cannot serve as trusted traveler escorts.

6. Trusted traveler procedures will be suspended at FPCONs CHARLIE and DELTA or when deemed necessary by the NSNPT CO.

7. An individual who has been denied an installation access credential, based on an adverse vetting return, cannot be escorted via trusted traveler.

8. An un-vetted foreign national may be escorted via trusted traveler.

9. Trusted traveler provisions apply at NSNPT off-installation locations that have a controlled perimeter, e.g. NUWC and NHCNE, unless specifically prohibited in writing.

(c) The NSNPT CO retains the flexibility to authorize trusted traveler escort privileges for unique categories and situations not addressed in this instruction. Public Private Venture (PPV) senior management personnel overseeing housing within the confines of NSNPT may be issued a CAC and approved to act as a sponsor for the purpose of supporting necessary maintenance personnel access to the installation.

c. Installation access credentials. The following credentials are accepted for installation access at NSNPT:

(1) Common Access Card (CAC) issued to active duty military and Department of Defense (DoD) civilian employees and contractors.

(2) Uniformed Services Identification (TESLIN) cards

(a) DD Form 2, United States Uniformed Services Card issued to retirees

(b) DD Form 2, United States Uniformed Services Card issued to reserve retirees

(c) DD Form 1173, Uniformed Services Identification and Privilege Card

(d) DD Form 1173-1, Department of Defense Guard and Reserve Dependent Identification Card

(e) DD Form 2764, United States DoD/Uniformed Services Civilian Geneva Conventions Identification Card

(3) DoD Civilian Retiree ID Card

(4) Non-DoD Federal Personal Identity Verification (PIV), and Personal Identity Verification-Interoperable (PIV-I) which includes HSPD-12 compliant credentials from:

(a) Department of State.

(b) Department of Treasury.

(c) Department of Justice.

(d) Department of Interior.

(e) Department of Agriculture.

(f) Department of Commerce.

(g) Department of Labor.

(h) Department of Health and Human Services.

(i) Department of Housing and Urban Development.

(j) Department of Transportation.

(k) Department of Energy.

(l) Department of Education.

(m) Department of Veterans Affairs.

(n) Department of Homeland Security.

(o) United States Postal Service.

(p) Individuals presenting the above credentials must be DoD sponsored and have a valid reason for installation access.

(q) Contract Background Investigators presenting a valid PIV card issued by the Office of Personnel Management (OPM) will be granted unescorted access.

(r) Personnel presenting Department of Energy Naval Reactors PIV cards will be granted unescorted access.

(5) Transportation Worker Identification Credential (TWIC). TWICs are tamper-resistant biometric credentials issued to all credentialed merchant mariners and workers who require unescorted access to secure areas of ports, vessels, and other facilities.

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

1. Possess a valid TWIC

2. Demonstrate a valid purpose for entry; examples may include government bill of laden (GLB) or commercial bill of laden (CBL), etc.

3. Be vetted and fitness determined

(6) Foreign Nationals (FN)

(a) NATO member country active duty military ID cards

(b) FN personnel International Travel Order accompanied by a valid passport

(7) NSNPT and tenant command issued passes and badges used to facilitate internal movement control, e.g. NUWC NAVSEA badges, are NOT valid installation access credentials.

d. Local installation access credentials

(1) Local installation access credentials are developed, issued, and tracked using the Defense Biometric Identification System (DBIDS). Vehicle passes are not issued however; vehicles are entered into the system and associated with the appropriate owner or driver.

(2) DBIDS is a Physical Access Control System (PACS) developed by the Defense Manpower Data Center (DMDC) which uses existing DoD records and information, digital images, and digital fingerprints to facilitate issuing credentials to individuals who are otherwise not authorized a DoD credential. The system is configured to DoD, U.S. Navy, and NSNPT unique requirements.

(3) The DBIDS system consists of the following elements:

(a) One Registration Workstation (RW) located in the Pass and ID (P&ID) office, which functions to register individuals and vehicles, issue DBIDS cards and visitor passes, and generate reports. The system consists of:

(b) Two Access Control Workstations (ACW), one located in the gate 1 guard house and one located in the gate 17 commercial vehicle station, which function to process access

transactions, verify identities, issue visitor passes, and serve as data host for handheld scanners. The system consists of (both locations):

(c) DBIDS handheld installation access credential scanners located at active installation ECPs.

1. DBIDS handheld scanners at gates 1, 2, and 7 (NHCNE) are wirelessly networked, via PSNet, to the gate 1 ACW.

2. DBIDS handheld scanners at gates 17, 23 (NUWC), and 32 (NUWC) are wirelessly networked, via PSNet, to the gate 17 ACW.

(4) DBIDS system accepted access credentials

(a) DoD issued CACs

(b) Federal agency cards (PIV) when appropriately barcoded

(c) DoD issued TESLIN cards

(d) DoD civilian retiree cards

(e) DBIDS cards

(f) DBIDS paper passes

(5) DBIDS card:

(a) DBIDS card can be issued for a period of up to two years.

1. Long term contractors ineligible for a CAC can be issued a DBIDS card for up to one year.

(b) DBIDS cards can only be issued at the P&ID office.

(c) Permissions can be set specifying days (of the week) and times when the card will be accepted for access.

(d) DBIDS card holders are not authorized to act as an escort.

(e) Vehicle limit allows the holder to drive only their own personal or assigned work vehicle.

(6) DBIDS paper pass:

(a) Passes issued at the P&ID office, using the RW, can be issued for up to 60 days.

1. Short term contractors will be issued only DBIDS passes for up to 30 days.

2. Passes issued at gates 1 or 17, using an ACW can only be issued for periods of one, two, or three days.

(b) DBIDS pass holders are not authorized to act as an escort.

(7) Handheld scanner operations

(a) Once a CAC, TESLIN, Rapid Gate, DBIDS credential is scanned by a gate guard:

1. The DBIDS system searches the local database. Local system searches typically take 1-2 seconds or less.

2. If a scanned credential is not located in the local DBIDS database the system executes a network search, via PSNet, into the Defense Enrollment Eligibility Reporting System (DEERS). This search can take up to 10 to 12 seconds.

a. If located, the record is copied into the local database.

e. Vetting

(1) Vetting is an evaluation of an applicant's character and conduct for approval, or denial, of the issuance of a DBIDS credential, or access list inclusion, for installation access. Upon completion, vetting is valid for 179 days. If further access time is required, a new vetting must be completed. Vetting includes three aspects:

(a) An individual(s) must have a valid purpose to enter NSNPT. This is established by the request submitted by a qualified sponsor (discussed in 3.e.(2)(b)).

(b) An individual(s) must be properly identity proofed – identity must be established by the presentation of a valid identity document.

1. A state issued driver's license or ID card submitted to establish identity must comply with the Real ID ACT of 2005 and not include words to the effect, 'not valid for federal use'.

2. All other acceptable identity documents are listed in TAB A.

(c) An individual(s) must have a favorable criminal background check completed.

1. A criminal background check consists of:

a. A background records check, by Social Security Number (SSN), in the Consolidated Law Enforcement Operations Center (CLEOC).

b. A search, by name, in the Department of Justice National Sex Offender Public Website (NSOPW).

(1) If NSOPW is off-line or a particular state is not returning results, a direct check of the state-maintained sex offender registry can be conducted.

c. A query in the National Criminal Information Center (NCIC) accessed via the Openfox web-based application.

2. Foreign Nationals (FN) are vetted by the Naval Criminal Investigative Service (NCIS) NSNPT field office.

a. FN resident aliens cannot be legally vetted by NCIS and will be vetted with U.S. nationals via CLEOC, NSOPW, and an National Law Enforcement Telecommunications System (NLETS) query.

b. FN citizens of Great Britain, Canada, Australia, and New Zealand are not normally vetted by NCIS due to the close relationship they share with the U.S. FN vetting requests for these individuals will be completed with U.S. nationals via CLEOC, NSOPW, and an NLETS query. NCIS must still be notified of the FN visit.

(2) Roles

(a) Identity proofing and vetting delegates. Those DoD civilian P&ID office employees, or military service members, who are assigned the duties of determining an individual(s) eligibility to be issued a NSNPT DBIDS installation access credential.

1. The CO will designate, in writing, those personnel who will perform identity proofing and vetting.

(b) Sponsor. Those approved individuals affiliated with the DoD eligible to take responsibility for verifying an applicant's need for and requesting vetting and access to the installation.

1. Valid sponsors include:

a. A uniformed service member (to include Guard and Reserve personnel on official orders) or U.S. Government employee with a valid CAC.

b. Privatized housing residents with locally issued NACVMS credentials are authorized to sponsor individuals onto the installation they are affiliated with, but sponsorship privileges should be limited to their particular housing area only.

c. Navy Federal Credit Union (NFCU) employees with locally issued credentials are authorized to sponsor NFCU affiliated individuals for the purposes of conducting NFCU business.

d. The NSNPT CO retains the flexibility to include sponsorship privileges for unique categories and situations not addressed in this instruction and not prohibited by higher headquarters instruction.

e. Military and DoD civilian retirees are not authorized to act as sponsor.

f. Contractors are not authorized to act as sponsors.

2. Vetting Request requirements. If any of these requirements are missing or incomplete the request will be returned to the originator for correction and re-submission

a. Vetting requests are only accepted from qualified sponsors.

b. Requests are only accepted in encrypted electronic format. In the event a qualified sponsor does not have the means to submit electronically, considerations can be made.

c. Requests must be submitted using the electronic excel spreadsheet template provided by P&ID personnel upon request.

d. The request must include start date, end date, social security number (SSN), last name, first name, date of birth (DOB), facility, company, sponsor, sponsor command, sponsor phone number, sponsor email, and on-base work or visit location.

(1) The facility block must always contain NAVSTA NEWPORT.

(2) The company block will contain be the company the individual works for or a brief description of the nature of the visit, e.g. "Personal Guest".

(3) The sponsor email and phone number must be a working email and phone number. Personal email addresses and phone numbers are not allowed. The only exceptions to this are for the U.S. Navy War College (NWC), the Senior Enlisted Academy (SEA), and the Naval Academy Preparatory School (NAPS) whose email addresses end with .edu; and the Navy Exchange (NEX) and Navy Federal Credit Union (NFCU) whose email addresses end with .org.

e. Since vetting requests contain Personal Identifying Information (PII) they must be emailed encrypted. If an originator cannot send encrypted messages they may either email the request password protected then send the password in a separate email or utilize the U.S. Army's AMRDEC website, https://safe.amrdec.army.mil/safe/.

(c) Unaffiliated individual guests. These individuals do not have normal access to NSNPT however, require access to perform necessary function(s). These guests fall into three categories:

1. Short term guests. Guests requiring installation access for part of a single day up to 30 days, e.g., family visits, retired civil service not in possession of a CAC, unaffiliated Navy Federal Credit Union (NFCU) patrons, sporting event participants and officials, etc.

2. Long term guests. Guests requiring installation access for a period greater than 30 days up to multiple years, e.g., long term permanent contract employees, volunteers, permanent food service employees, transportation providers, etc.

3. Commercial deliveries. Commercial vendors making a single visit for the purpose of delivering commercial goods and services, e.g., supply deliveries to a visiting unit(s), commercial furniture deliveries, construction deliveries, etc. These individuals normally receive only a one day pass however, they may be issued a pass valid for up to three days. All commercial deliveries are processed through the gate 17 commercial vehicle station.

(3) Vetting capabilities. Vetting can be accomplished by either of two existing entities.

(a) The Commander Navy Region Mid-Atlantic (CNRMA) Personnel Screening Center (PSC)

1. Due to the large volume of vetting requests, the bulk of the NSNPT vetting requests are submitted to the PSC for vetting.

2. All vetting requests must be submitted to the PSC a minimum of 5 working days in advance. This minimum advanced period does not include the date of request submission or the start date. Requests received after normal P&ID working hours will not be processed until the following day, making the following day the effective receipt date for determining required request lead time.

3. Upon completion, all vetting results, including those received from other CNRMA installations, are published in the Visitor Access Control List (VACL). This document is available daily, in electronic format, accessible on the CNRMA network share drive.

(b) Locally at the NSNPT P&ID Office in building 1377

1. Small numbers of vetting requests can be accomplished locally.

2. All locally performed vetting and results are entered into the NSNPT Walk-In database using locally developed Microsoft Access tools, a CNRMA developed and maintained Microsoft Access database accessible on the CNRMA network share drive.

3. The PSC adds the local vetting results from the NSNPT Walk-In database to the VACL daily.

4. Local vetting is performed for individuals requesting installation access at the gate 17 commercial visitor station and for emergent, short lead (not within the minimum 5 day advance period) visitor requests received at the P&ID office.

5. Vetting results are categorized as:

a. Cleared – The individual is eligible to be issued a DBIDS NAVSTA Newport installation access credential.

b. On Hold – incomplete vetting results were returned. Individuals with incomplete vetting results will not be issued a DBIDS credential until a result of cleared can be determined.

c. Denied. Individual is ineligible to be issued a DBIDS credential or be escorted via Trusted Traveler. When denied, an individual is discreetly informed of the denial (if present) and provided an informational document with information on the waiver and appeal process, see TAB B. Information on the reason for a denial cannot be provided to any individual or agency.

(1) Waiver and appeals process: Individuals who have been denied access may appeal or request a waiver in writing from the CO. When reviewing criminal history to make a waiver determination, both adverse information and mitigating factors will be considered. The individual requesting a waiver will be notified in writing of the decision within 30 days of package submission.

(2) Denial Criteria which may not be waived.

(a) Identification in the Foreign Fugitive File.

(b) Identification in the Immigration Violator File.

(c) Registered in the National Sex Offender Registry Database. Sex offenders identified through the National or State Sex Offender Registry Databases are permanently prohibited from accessing NSNPT or any other Navy installation or facility.

(d) Identified as a known or appropriately suspected terrorist.

(e) Felony convictions for Rape, Child Molestation, Trafficking in Humans, Espionage, Sabotage, Treason, or Terrorism.

(3) Denial Criteria which may be appealed or waived.

(a) Any felony conviction, other than those listed in "3.e.(3)(b)5.c.(1)(e)" above, within the past 10 years. Arrests for a disqualifying event without disposition (conviction, dismissal, not guilty or acquittal) more than 10 years old are not grounds for denying access.

(b) Individuals identified in the Violent Person Crime File. The Violent Persons File lists individuals with a violent criminal history and persons who have previously threatened law enforcement.

(c) Individuals with active wants or warrants.

(d) Individuals with a current debarment issued by the NSNPT CO or another DoD CO.

d. Debarred. Installation access privilege has been permanently or temporarily revoked by the NSNPT CO or by the CO at another DoD installation.

e. Clear-No Driving. Individual(s) can be issued an installation access credential however, cannot operate a motor vehicle while on the installation for one, or more, of the following reasons.

(1) Driving privilege revoked or suspended. An individual(s) has been barred from operating a motor vehicle on board NSNPT by the CO for a designated period of time. Driving privileges revoked at another DoD installation will be enforced at NSNPT.

(2) Conviction of operating a motor vehicle while under the influence of an illegal drug or alcohol. This "No Driving" status will be for a period of one year from the disposition date of the offense. If charges are in a pending status, driving status will be "On-Hold" (effectively no driving) until a disposition is reached or one year from the date charged.

f. Other installation access control considerations:

(1) Forgotten, lost (or confiscated), or stolen installation access credential

(a) ID card forgotten at place of work or residence

1. The individual must confirm their identity by providing identification documentation consistent with enclosure (1), be verified in DBIDS, then issued a temporary pass.

2. If an individual is unable to provide the required identity proofing documentation or cannot be located in the DBIDS system then other means of installation access will need to be sought by the individual such as escort by a qualified trusted traveler.

(b) Lost (or confiscated) ID card

1. The individual must confirm their identity by providing identification documentation consistent with enclosure (1), be verified in DBIDS, then issued a temporary pass.

2. The ID card will be marked as lost in the DBIDS system.

3. If an individual is unable to provide the required identity proofing documentation or cannot be located in the DBIDS system then other means of installation access will need to be sought by the individual such as escort by a qualified trusted traveler.

(c) Stolen ID card

1. The individual must confirm their identity by providing identification documentation consistent with enclosure (1) and be verified in DBIDS.

2. An NSNPT Police unit will be requested to respond to the reported stolen ID card per Police PPRs (PPR) and SOPs.

3. Upon completion of processing with the responding NSNPT Police unit, the individual may be issued a temporary pass.

4. The ID card will be marked as lost in the DBIDS system.

5. If an individual is unable to provide the required identity proofing documentation or cannot be located in the DBIDS system then other means of installation access will need to be sought by the individual such as escort by a qualified trusted traveler.

(2) NUWC. As the entire NUWC compound is classified as a level one restricted zone, special considerations are necessary for NUWC access.

(a) There are two separate, unrelated, considerations to access the NUWC compound at both NSNPT gates 23 and 32.

1. Installation access. Any individual(s) entering NSNPT through gates 23 or 32 must present a valid installation access credential. Any individual(s) not in possession of such a credential, and not otherwise restricted from installation access, may be considered eligible for access via the trusted traveler program.

2. Individual movement control within the NUWC level one restricted zone. The issuing of credentials for internal movement control within the NUWC level one restricted zone is under the cognizance of the NUWC Commanding Officer. As the perimeter of the NUWC level one restricted zone coincides with the NUWC compound perimeter (for installation access considerations), the gate 23 and 32 sentries will validate all individuals possess a current and valid NUWC level one restricted zone movement credential, in addition to a current and valid installation access credential. Failure of an individual to present either of these documents will result in access denial and turn-around, unless escort via trusted traveler is being utilized, in which case only a level one restricted zone movement credential will be required.

a. NUWC is responsible for providing NSNPT Security a description of all documentation used to facilitate internal movement control within the NUWC level one restricted zone and to ensure all descriptions are maintained up to date.

(3) Morale Welfare & Recreation (MWR) Events. MWR frequently hosts and supports events at MWR facilities. Frequently, these events involve large numbers of unaffiliated individuals. The NSNPT CO may authorize modifications and exceptions to normal vetting procedures in support of MWR events.

(a) These events include but, are not limited to:

1. Wedding ceremonies, receptions, and related catering appointments

2. Retirement ceremonies and receptions

3. Birthday, holiday, or special event parties

4. League sporting events (e.g. bowling)

5. Special seminars, lectures, guest speakers, etc.

(b) MWR may request unaffiliated and un-vetted individuals be placed on the installation access provided the sponsor of the event has acknowledged, in writing, the acceptance of full responsibility for the actions of their guests. This acknowledgement will be documented and maintained by security.

(c) These vetting procedure exceptions will not apply to general public visitation (GPV) events and guests of marina patrons. GPV events will either follow vetting procedures, outlined in this instruction, or be controlled by the implementation of a Special Event Antiterrorism (SEAT) plan. Guests of marina patrons will be subject to vetting procedures per the guidance in this instruction.

(4) Access control at each Force Protection Condition (FPCON).

(a) FPCONS NORMAL, ALPHA, and BRAVO. There are no deviations from guidance in this instruction at FPCON's NORMAL, ALPHA and BRAVO.

(b) FPCON CHARLIE. Discontinue use of trusted traveler program.

(c) FPCON DELTA. Limit access to mission essential personnel and other personnel as determined by the NSNPT CO.

(5) Mission Essential Personnel (MEP). At times as the CO deems necessary, installation access will be limited to MEP only. The CO designates those individuals deemed to be mission essential.

(6) Officer Training Command Newport (OTCN) Graduations. Unless covered by the OTCN and NSNPT AT plans, by a SEAT plan, or authorized by the NSNPT CO; guests for OTCN graduations must be vetted per guidance in this instruction.

(7) Naval Academy Preparatory School (NAPS)

(a) Athletic Events. Unless covered by the NAPS and NSNPT AT plans, by a SEAT plan, or authorized by the NSNPT CO; guests, to include but not limited to NAPS parents, visiting team members, visiting team member parents, sporting officials, etc. must be vetted per guidance in this instruction.

(b) Graduations. Graduations, and related events, held on board NSNPT; unless covered by the NAPS and NSNPT AT plans, by a SEAT plan, or authorized by the NSNPT CO; all guests must be vetted per guidance in this instruction.

(c) All other events. Unless covered by the NAPS and NSNPT AT plans, by a SEAT plan, or authorized by the NSNPT CO; guests must be vetted per guidance in this instruction.

(8) Unaffiliated Distinguished Visitors (DV). Periodically, unaffiliated DVs will be invited to the installation for a variety of events. Sensitivity to the status of the DV will be maintained however, vetting requirements will not be deviated from without authorization from the NSNPT CO.

(a) Vetting will be waived for publically elected local, state, and federal officials currently in office.

(b) Vetting will be waived for support staff of publically elected state and federal officials currently in office.

(c) Vetting will NOT be waived for support staff of locally elected officials currently in office.

(9) Local, State, and Federal law enforcement (LE); and Fire Fighting (FF) officials.

(a) These officials will be authorized installation access for official business, without a pass, provided they present current and valid credentials and are driving an official marked or unmarked vehicle.

(b) These officials will be authorized installation access for mutual aid support, without a pass. The Regional Dispatch Center or Local Dispatch Center should provide advanced notification to gate sentries prior to arrival.

(10) Media Representatives, to include but, not limited to, broadcast, written, electronic, etc.

(a) If a member(s) of the media arrives at the P&ID, announced or unannounced, no statements will be made nor any questions answered. All representatives will be directed to the NSNPT Public Affairs Office (PAO).

(b) No installation access credential will be issued without the explicit authorization of the SECDIR or the NSNPT CO.

(11) Navy Federal Credit Union (NFCU). Unaffiliated individuals with NFCU accounts may be authorized installation access. NFCU must provide vetting requests for these patrons. This will provide verification that the individual(s) have NFCU accounts. Upon a favorable vetting a short term pass can be issued, not to be valid longer than one day.

(12) Legal servicing and vehicle repossessions. Any individual arriving at the P&ID seeking installation access for the purpose of serving legal documents or repossessing a vehicle will be referred to the NSNPT Judge Advocate General (JAG). No other information will be provided to these individuals.

(13) Transportation Services

(a) Definitions

1. Transportation Service Provider (TSP). An organization which provides transportation services for any individual(s), is available to the general public (or any subset of the public, e.g. public school bus service), whether reimbursement is provided for the transportation or not. TSPs include but, are not limited to taxis, Uber, Lyft, Rhode Island Public Transit Authority (RIPTA), school bus service, etc. Privately contracted transportation drivers, to include tour bus drivers (contracted for specific events or jobs) and limousine services will not be considered TSPs.

2. Single Source Coordinator (SSC). An individual(s) within an organization at NSNPT who coordinates driver installation access for one, or more, TSPs.

3. RIDE. The RIPTA, Americans with Disabilities Act compliant, transportation service. RIPTAs RIDE service provides transportation for some employees on NSNPT.

(b) Taxi, Uber, and Lyft. The Navy Exchange (NEX) is the SSC for, and registers all taxi, Uber, and Lyft drivers; and forwards vetting requests for these individuals to the P&ID office. In addition to the normal vetting process all taxi, Uber, and Lyft drivers will have their driver's licenses and vehicle registrations checked. Upon a favorable vetting result, these drivers may be issued a DBIDS card for up to one year. If a driver's employment is terminated, for any reason, it is the responsibility of the NEX to notify the P&ID office so the individual's DBIDS credential can be terminated.

(c) RIDE. Since there is no single entity that makes exclusive use of RIDE drivers on board NSNPT, there are not SSCs for all individuals making use of RIDE services. The major users are the Naval War College (NWC), Ney Hall Galley, and NAVFAC. RIDE drivers will be

vetted and, upon a favorable return, be issued a DBIDS card for up to one year or until termination of their employment with RIPTA provided the driver's vetting is maintained current. If a driver's employment is terminated, for any reason, it is the responsibility of the sponsor or RIPTA to notify the P&ID office so the individual's DBIDS credential can be terminated.

(d) Public school busses. The School Liaison Officer (SLO) is the SSC for public school bus drivers and will be responsible for submitting drivers for vetting. Public school buses will be allowed access to NSNPT for the sole purpose of picking up and dropping off students who reside on the installation. Upon a favorable vetting DBIDS cards may be issued to the drivers for the duration of the school year or until termination of employment. If a driver's employment is terminated, for any reason, it is the responsibility of the SLO to notify the P&ID office so the individual's DBIDS credential can be terminated

(14) Limousine services. Affiliated individuals desiring to make use of limousine services will be responsible for the vetting request submission of the drivers and the coordination of the drivers obtaining an appropriate installation access credential.

(15) Vehicle towing and roadside assistance.

(a) Individuals requiring towing or roadside assistance must contact the P&ID office either via email, telephone, or in person to report the anticipated arrival of the service vehicle and establish the actual need for installation access.

(b) Once the service provider requested arrives at the P&ID office, the driver will be vetted and, upon a favorable return, be issued a temporary pass, valid for only a reasonable time in which to render the requested service(s), not to exceed one day.

(c) After hours towing service installation access will be handled per NSNPT Security Law Enforcement SOPs and PPRs.

(16) Motorcycles. Personnel desiring to operate motorcycles on NSNPT must complete the required motorcycle safety course. Affiliated personnel must present documentation of the safety course prior to their motorcycle being registered in CLEOC.

(17) Vehicles transporting ordnance. Any vehicle transporting ordnance must be escorted by NSNPT police while driving onboard NSNPT, per NSNPT LE SOPs and PPRs.

(18) Terminated employees. Terminated employees, to include but not limited to terminated DoD employees, terminated contractors, terminated sub-contractors, etc.; with no other military affiliation, are not authorized to be present on board NSNPT. Terminated employees will be immediately reported and their CAC, DBIDS card, or DBIDS pass invalidated to prevent any further installation access.

(19) Installation access list. When a large group of vetted, unaffiliated guests will be accessing the installation on a single day, pass issuance would overwhelm the capacity of the NSNPT Pass office. In these circumstances an access list may be generated in lieu of a pass.

Guests will be required to provide a current and valid identification, to a gate sentry, and matched to the installation access list prior to granting access.

TABS:
TAB A: List of Acceptable Identification Documents
TAB B: Denial Appeal and Waiver Procedures

TAB A
Acceptable Identity Proofing Documents

1. U.S. Passport or Passport Card
2. Permanent Resident Card or Alien Registration Receipt Card
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa (MRIV)
4. Employment Authorization Document (Card) that contains a photograph (Form I-766)
5. In the case of a nonimmigrant alien authorized to work for a specific employer incident to status: a. Foreign passport; and b. Form I-94 or Form I-94A has the following: (1) Bearing the same name as the passport; and (2) An endorsement of the alien's nonimmigrant status, as long as the period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form.
6. Driver's license or ID card issued by a Real ID Act compliant state or outlaying possession of the U.S., provided it contains a photograph and biographic information such as name, date of birth, gender, height, eye color, and address. Licenses or IDs possessing "NOT APPLICABLE FOR FEDERAL PURPOSES" will not be accepted.
7. State-issued Enhanced Driver's licenses
8. Driver's license issued by the U.S. Department of State
9. Border Crossing Card (From DSP-150)
10. Identification card issued by Federal, State, or local government agencies, provided it contains a photograph and biographic information such as name, date of birth, gender, height, eye color, and address.
11. Veteran Health Identification Card (VHIC) issued by the Department of Veterans Affairs
12. Department of Homeland Security "Trusted Traveler" Cards (Global Entry, NEXUS, SENTRI, FAST)
13. U.S. Certificate of Naturalization or Certificate of Citizenship (Form N-550)
14. School identification card with a photograph
15. Persons under the age of 18 who are unable to present a document listed above may present one of the below documents. a. School record or report card b. Day care or nursery school record c. Birth certificate (original or certified copy)
16. Native American Tribal Photo ID cards
17. U.S. Coast Guard Merchant Mariner Credential (MMC) or Merchant Mariner's Documents (MMD)
18. Other documents that may be provide for identity proofing purposes, but must be accompanied by a second form of ID with photograph and biographical information. a. Social Security Number card b. Original or certified copy of a birth certificate issued by a state, county, municipal authority, or outlying possession of the U.S. bearing an official seal. c. Certification of birth Abroad issued by the U.S. Department of State (Form FS-545) d. Certification of Report of Birth issued by the U.S. Department of State (Form DS-1350 e. Voter's Registration Card

TAB B

WHAT TO DO IF YOU ARE "DENIED" BUT THINK YOU DON'T MEET THE CRITERIA

Contractors who are "DENIED" due to their Criminal History get an immediate review to verify that the denial is proper. Denials are not posted until they have been reviewed. If your access request was denied and you believe that you don't meet the criteria, follow the instructions below. Since the Criminal History was determined by name and date of birth check on NCIC, and cross verified with SSN, it's possible that a denial based on these factors could be mistaken.

Instructions:

1. The applicant should request his/her **OWN** record by submitting a written request and fingerprint cards to the FBI and paying $18.00. The instructions on how to do so are at:

http://www.fbi.gov/about-us/cjis/identity-history-summary-checks/order

2. Once the results are received from the FBI, the entire report should be mailed to:
Regional Security, (Attn: Personnel Screening Center)
Norfolk Naval Station
1510 Gilbert St.
Building N-26, Norfolk, VA 23511

3. Ensure that you include contact information so that the Screening Center can get in touch with you.

4. **DO NOT CALL** REGIONAL SECURITY - by law we cannot and will not tell you specifically "why" you're denied.

WHAT TO DO IF YOU ARE "DENIED" BUT THINK THERE ARE EXTENUATING CIRCUMSTANCES

- ❑ Explain the extenuating circumstances to your company.
- ❑ Your Company may forward the explanation to their Trusted Agent (TA) or Authorizing Official (AO). This is the Government point of contact to whom your name was submitted for sponsorship.
- ❑ The **TA** or **AO** will either **choose whether or not** to make an appointment with the Installation Commanding Officer to explain:
    - o Why they need you to work,
    - o What mitigations the command is prepared to put in place, or;
    - o What mitigations the company will put in place
- ❑ If the CO or XO decides to grant an exception to the denial criteria, the Regional Security Officer will be notified of that decision. If not, the "DENIED" status will remain in effect.

DENIAL CRITERIA FOR MID-ATLANTIC BASES

- ➢ Felony conviction of any type within 10 years, or a felony arrest that has not been adjudicated yet (includes "Deferred Findings").

- ➢ Sex Offender Registry or Sex Offense conviction is permanent denial per OPNAVINST

- ➢ Barment from one Navy Installation includes reciprocal barment from all Navy Installations.