



DEPARTMENT OF THE NAVY  
NAVAL SUPPORT ACTIVITY WASHINGTON  
1411 PARSONS AVENUE SE, SUITE 303  
WASHINGTON NAVY YARD 20374-5003

NSAWINST 5530.14  
N3  
4 Oct 13

NAVAL SUPPORT ACTIVITY WASHINGTON INSTRUCTION 5530.14

From: Commanding Officer, Naval Support Activity Washington

Subj: NAVAL SUPPORT ACTIVITY WASHINGTON INSTALLATION ACCESS  
CONTROL

Ref: (a) DoD DTM 09-012  
(b) DoDI 1000.13  
(c) DoDI 2000.16  
(d) SECNAV M-5210.1  
(e) OPNAVINST 5530.14E  
(f) CNICINST 5530.14  
(g) OPNAVINST 1752.3  
(h) CNICNOTE 5530 cf Feb 11  
(i) BUPERSINST 1750.10  
(j) DoD 5200.08-R  
(k) DoDI 5200.08  
(l) DoDD 2000.12 - AT Program  
(m) COMUSFLTFORCOM OPORD 3300-09  
(n) DoD O-2000.12-H - AT Handbook  
(o) SECNAV memo of 7 Oct 08  
(p) SECNAV M-2510.1

Encl: (1) Commanding Officer, Naval Support Activity Washington  
Installation Access Control Program Guidance

1. Purpose. Provide and promulgate standardized installation access control policy and guidance for the Commanding Officer, Naval Support Activity Washington (NSAW), in accordance with (IAW) references (a) through (p). This is a new instruction and should be reviewed in its entirety.

2. Background

a. Scope. This instruction defines the responsibility of Installation Commanders and Commanding Officers (CO) (both are hereafter referred to as 'CO') in establishing, implementing, and

4 Oct 13

sustaining scalable Base Operating Support (BOS) related access control procedures. These procedures are based on guidance from Commander, U.S. Fleet Forces Command (COMUSFLTFORCOM); Commander, Navy Installations Command (CNIC); Required Operational Capability (ROC) Levels; and Force Protection Conditions (FPCON).

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

c. Applicability. This instruction applies to all Navy installations within the NSAW Area of Interest (AOI). This instruction is applicable to Navy personnel, including active and reserve components, Navy civilians, Navy families, Navy and non-Navy tenants, contractor personnel, visitors, guests, and foreign national personnel.

3. Policy. In accordance with references (a) through (o), the primary objectives of the NSAW Access Control Program are as follows:

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

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

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

(1) Have a valid purpose to enter;

(2) Be identity-proofed;

(3) Be identity-vetted; and

(4) Possess a valid access credential.

d. The following sources will be queried to vet the claimed identity and determine access:

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

(2) The Terrorist Screening Database

(3) The Sex Offender Registry

- (4) The Foreign Visitor System - Confirmation Module (FVS-CM)
- (5) The Department of Homeland Security (E-Verify)
- (6) The Department of Homeland Security (U.S. VISIT)
- (7) The Department of State Consular Checks (non-U.S. citizen)

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

4. Access Authorization and Requirements. Access to Navy installations is not a right, and is within NSAW 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; proper vetting has occurred; and persons are authorized by the Installation CO. At a minimum, consideration should be given to threat, criticality, and vulnerability in the risk assessment process.

a. All unescorted persons entering NSAW installations must have a valid purpose to enter, must be identity-proofed and vetted, and be issued, or in possession of, an authorized and valid access credential. Escorted personnel do not have the same background check requirements. Special events that are covered under an Anti-Terrorism (AT) plan (e.g., Force Protection Special Event (FPSE), CNO Arrivals, 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 the NSAW AT plan.

Active Duty  
Reserve

CAC ID  
CAC ID

4 Oct 13

Dependents (age 10 or older)	Military ID
Military Retirees	Military ID
Civil Service Employees	CAC ID

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

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

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

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

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

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

#### 5. Assumptions

a. The Navy Commercial Access Control System (NCACS) will be the primary access control system for contractors and vendors. Vetting for NCACS participants will occur every 92 days, for nonparticipants, every 90 days. Additionally, nonparticipants must receive an installation pass daily.

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

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

6. Responsibilities. All NSA Washington fence lines will incorporate access control procedures required by this Access Control Program.

a. Commanding Officer, NSAW shall:

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

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

(3) Is granted the authority and responsibility to protect personnel, equipment, and facilities subject to their control. Neither this instruction nor the access control program shall detract from, or conflict with, the inherent and specified authorities and responsibilities of the Installation CO.

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

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

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

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

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

  
M. L. ULMER

Distribution:  
Electronic only, via CNIC GATEWAY PORTAL, NSA Washington Site,  
<https://g2.cnic.navy.mil/TSCNRNDW/NSAWASHINGTONDC/default.aspx>

4 Oct 13

**Commanding Officer, Naval Support Activity Washington  
Access Control Program Guidance**

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

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

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

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

b. NSAW access control policy addresses the following:

(1) Types of Access

(a) Unescorted individuals

(b) Escorted individuals

(c) Special event access. NSAW does not require full background checks on guests of special events (Catering & Conference Center, Admiral Gooding Center, Naval History & Heritage Command). The staff at the VCC will run a CLEOC check to make sure the guest is not barred from NSAW (or any other installations) and check the Sexual Offender Registry.

1. No later than five business days prior to the event, NSAW requires a list with the following information:

- a. Full name
- b. Contact number
- c. Date(s) access required
- d. Purpose for access
- e. Vehicle type
- f. Vehicle plate number
- g. State issued ID number
- h. Sponsor
- i. Sponsor Contact information

2. These names will be printed out and posted at gates the day(s) access is required. Lists will not contain any PII.

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

- (a) Escort qualifications, responsibilities, and authorizations.
- (b) Sponsorship qualifications, responsibilities, and authorizations.

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

## 2. Procedures

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

**NOTE:** Contractors are not authorized to serve as escorts.

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

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

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

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

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

**NOTE:** Contractors are not authorized to serve as sponsors.

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

(1) The VCC will ensure that all visitors have a completed National Crime Information Center (NCIC)/Washington Area Law Enforcement System (WALES), Sex Offender Registration and Notification Act (SORNA), Terrorist Screening database, and a local no-entry and barment list check.

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

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

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

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

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

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

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

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

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

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

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

(2) **Step 2:** NSAW VCC submits request data to JBAB VCC for vetting.

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

(4) Cleared

(a) Step 4A: The visitor can be issued a visitor pass/badge. Visitor passes should be issued for the duration of the visit, but not to exceed 30 days. Pass and ID clerks will be responsible to verify the person receiving the visitor pass has the proper credentials listed in Table 1.

(5) Denied

(a) Step 4B: The visitor **WILL NOT** be issued a visitor pass/badge. Pass and ID clerks will give the visitor the following:

You have been denied access to Naval Support Activity Washington.

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

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

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

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

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

**NOTE:** Unauthorized dissemination of criminal history record information to any agency or person can result in criminal and civil penalties

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

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

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

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

**NOTE: Off Hours:** Delivery personnel, vendors, and visitors will not be granted access until vetted at the VCC. Additionally, during off hours they can follow the escort procedures.

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

(1) Only personnel designated by the Commanding Officer shall perform access control duties that include:

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

List of Personal Status, Access Credential, and Required Vetting

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

<u>Status</u>	<u>Access Credential</u>	<u>Vetting</u>
Active Duty Military	CAC	Not required
Reserve	CAC	Not required
Foreign Military TDY	CAC	Not Required
DON Civil Service	CAC	Not Required
Dependents	Military ID	Not required
Military Retirees	Military ID	Not required
Foreign Military Dependents	Military ID	Not Required
Law Enforcement	LE Credential	Not required
Transportation Worker	TWIC	Not Required
Other U.S. Government	Identification Credential USG-issued Federal PIV Credentials	Not Required
Unescorted Family Members Non-Dependant	Visitor Pass	Required
Unescorted visitor	NCACS/Day Pass	Required
Contractors	NCACS/Day Pass	Required
Vendor	NCACS/Day Pass	Required
PPV Housing	Badge	Required
Volunteers	Badge	Required
Dependent's Agent	Badge	Required
Merchant Seaman	Visitor Pass	Required
Student	Badge	Required
MWR	Visitor Pass	Required
Navy Guest	Visitor Pass	Required
Randolph Sheppard	Badge	Required
Act blind vendors		Required
Taxi drivers	Badge	Required

Note: Taxi drivers are sponsored by the NEX and pay a service fee, they do not participate in NCACS.

**Note: Law Enforcement**

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

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

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

NSAWINST 5530.14  
N3  
4 Oct 13

Table 1

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

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

VISITOR CONTROL CENTERS

NSAWINST 5530.14

N3

4 Oct 13

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

Washington Navy Yard, Washington DC

M-F 0530-1630 (202) 433-3017  
(202) 433-3735  
(202) 433-3738

NSF Carderock, West Bethesda, MD

M-F 0600-1600 (301) 227-1500  
(301) 227-1501