



DEPARTMENT OF THE NAVY
COMMANDER, NAVY INSTALLATIONS COMMAND
716 SICARD STREET, SE, SUITE 1000
WASHINGTON NAVY YARD, DC 20374-5140

Canc: Jun 2013
CNICNOTE 5530
N3
5 Jul 2012

CNIC NOTICE 5530

From: Commander, Navy Installations Command

Subj: NAVY COMMERCIAL ACCESS CONTROL SYSTEM WITHIN CONTINENTAL
UNITED STATES REGIONS, NAVY REGION HAWAII, AND JOINT
REGION MARIANAS

Ref: (a) OPNAVINST 5530.14E
(b) DTM 09-012, Interim Policy guidance for DoD Physical
Access Control, 30 Sept 2010
(c) DTM 08-006, DoD Implementation of Homeland Security
Presidential Directive-12 (HSPD-12), 27 Sept 2011
(d) FIPS 201, Personal Identity Verification of Federal
Employees and Contractors, 23 Jun 2006
(e) DTM 08-003, Next Generation Common Access Card
(CAC) Implementation Guidance, 27 Sept 2011
(f) CNICINST 5530.14

Encl: (1) Navy Commercial Access Control System Standard
Operating Procedures

1. Purpose. To update documentation of Navy Commercial Access Control System (NCACS) terminology and expectations of use of the system application. The program has been implemented and is currently operational throughout the Navy regions in the continental United States, Navy Region Hawaii, and Joint Region Marianas.

2. Background

a. References (a) through (f) provide overarching Navy policy, guidance, information, procedures, and responsibilities for the Navy Physical Security and Law Enforcement Program. NCACS is an operational program for Navy security and access control policy. It operates on the principle of person validation, rather than cargo inspections. During force protection conditions (FPCON) normal and alpha, verification of identity and current needs for physical access is conducted with each access request.

b. The NCACS identity management and perimeter installation access control solution is specifically designed to manage recurring vendors, contractors, suppliers, and other service providers who are not authorized a Common Access Card (CAC). It uses the following concept of operations:

(1) NCACS is a voluntary program in which participants who enroll and are subsequently approved for access by the installation are not required to obtain a new pass from the base Pass and Identification Office for each visit, and other than during random anti-terrorism measures or elevation of FPCON, no commercial vehicle inspection is required.

(2) An NCACS credential is issued and base access is granted once the enrollee passes vetting standards. Enclosure (1) provides specific vetting standards and credential issuance procedures. This includes a check of the local and region barment database, and the National Crime Information Center and Sex Offender Registration and Notification Act database.

(3) Vetting, maintenance of databases, the creation of credentials, and the technology required for authentication are currently being provided by a service contractor under the NCACS program.

(4) Installation and Region costs to implement NCACS are minimal and consist of providing the service contractor with electrical power, analog phone lines, and space for registration station kiosks at the Pass and Identification Offices or other locations approved by Commander, Navy Installations Command (CNIC).

(5) The majority of the NCACS costs are borne by the vendors and contractors who require access to the installation and choose to participate in the program through fees paid to the service contractor.

(6) Costs to vendor participants are recaptured through increased productivity of their employees through the reduction of waiting times and multiple visits to the Pass and Identification Offices for one-time/day passes and throughput at Entry Control Points (ECP).

3. Policy. NCACS shall accomplish the following:

a. Provide the single identity management and perimeter installation access control solution and credential for the access management of vendors, contractors, suppliers, and service providers who are not authorized a CAC in accordance with this notice and standard operating procedures (SOPs) and references (a) through (f).

b. Standardize the process across the CNIC claimancy to enroll, vet, credential, and electronically control access privileges of non-CAC vendors and contractors requesting installation access.

c. Improve efficiency and effectiveness at Pass and Identification Offices through a reduction in the issuance of routine business passes and other locally produced credentials.

d. Comply with best security practices and Defense Information Assurance Certification and Accreditation Process information assurance controls that prohibit the storage of personally identifiable information on mobile devices.

e. Ensure electronic perimeter installation access control management is in or near real time of enrolled participants, that the privileges are granted for a specific time of day, day of the week, and installation, and that they are current at all times. Privileges of NCACS vendors and contractors may be extended to more than one installation, if authorized, and any applicable enrollment fees shall be paid to the NCACS service contractor.

f. Program Support

(1) NCACS program performance and administration will be accomplished through a service contractor.

(2) The current service contractor is Eid Passport, Incorporated, Portland, Oregon.

(3) Eid Passport, Incorporated will utilize the *RAPIDGate* system to accomplish vetting, credentialing, and authentication.

(4) In the event that new or additional service contractors are selected and approved to administer NCACS or provide additional CNIC-approved NCACS credentials, public notice shall be provided.

JUL 5 2012

4. Responsibilities

a. Each region or installation is responsible for establishing a NCACS point of contact and providing the individual's contact information to CNIC Headquarters (HQ) N3AT via email to scott.silk@navy.mil and sharon.gibson@navy.mil. These designated personnel will participate in regularly scheduled teleconferences and serve as the points of contact for day-to-day management of NCACS.

b. Regions are responsible for ensuring that each installation complies with this notice and SOP and for establishing NCACS SOPs and posting them on the CNIC Gateway 2.0 (G2) NCACS website at: <https://g2.cnic.navy.mil/tscnichq/N3/N3AT/SOPs/Forms/AllItems.aspx>. Enclosure (1), Navy NCACS SOP, contains the minimum mandatory requirements for NCACS.

c. Installations are responsible for:

(1) Maintaining a one-day visitor pass program for those non-CAC vendors and contractors who choose not to enroll in the NCACS.

(2) Ensuring, per local SOP, that visitor passes are issued in compliance with Federal, Department of Defense (DoD), Department of Navy (DON), and CNIC guidance.

(3) Assistance for Regional and Installation responses to inquiries shall be directed to CNIC HQ for help with Frequently Asked Questions (FAQs) and Public Affairs Guidance (PAG).

5. Forms and Reports. The NCACS service contractor shall produce a Monthly Activity Report for each installation, which provides an overview of active companies, participants, ingresses by ECP, and other useful information for purposes of managing the program.


W. D. FRENCH
Vice Admiral, U.S. Navy

Distribution:

Electronic only, via CNIC Gateway 2.0

<https://g2.cnic.navy.mil/CNICHQ/Pages/Default.aspx>

**NAVY COMMERCIAL ACCESS CONTROL SYSTEM
STANDARD OPERATING PROCEDURES**

1. Purpose. To establish and prescribe procedures for access control to Commander, Navy Installations Command (CNIC) bases in the continental United States (CONUS), Hawaii, and Guam via entry control points (ECP) equipped with Navy Commercial Access Control System (NCACS), in accordance with policies, directives and instructions listed in Appendix A below.

2. Background

a. General. NCACS is an enterprise identity management and perimeter installation access control solution implemented within CONUS Regions, Navy Region Hawaii, and Joint Region Marianas. NCACS is designed to manage vendors, contractors, sub-contractors, suppliers, and service providers (vendors and contractors) not authorized to receive a Department of Defense (DoD) Common Access Card (CAC), regardless of how they access the installation, e.g., on foot, by privately owned vehicle, delivery vehicle, semi-truck, or any other method. NCACS participants will be enrolled, vetted, and credentialed, and their access privileges to CNIC installations will be regularly and electronically updated, verified, and documented upon each ingress at all perimeter ECPs.

b. Objective and Goals. NCACS is intended to:

(1) Enhance installation safety and security by using a common system across the CNIC enterprise to enroll, authenticate, credential, authorize, and manage access privileges of vendors and contractors coming aboard CNIC installations.

(2) Enhance efficiency and effectiveness at Pass and Identification Offices through improved business processes and a significant reduction in the issuance of contractor/business passes and other locally produced credentials.

(3) Enhance efficiency and effectiveness at all perimeter ECPs, specifically through the improved management of vendors and contractors, their vehicles, and throughput of all vehicles coming aboard CNIC installations.

c. Voluntary

(1) Participation in NCACS is not mandatory. The standard operating procedures (SOPs) outlined here do not eliminate other traditional methods of permitting access to Navy installations such as daily local passes, CAC, and other approved Federal credentials.

(2) In the event any CNIC activity develops a contractual requirement that includes vendor and contractor access to an installation, the Statement of Work or Performance Work Statement should include the following interim provision:

"Commander, Navy Installations Command (CNIC), has established the Navy Commercial Access Control System (NCACS), a standardized process for granting unescorted access privileges to vendors, contractors, suppliers, and service providers not otherwise entitled to the issuance of a Common Access Card (CAC) who seek access to and can provide justification to enter Navy installations and facilities. Visiting vendors may obtain daily passes directly from the individual Navy installations by submitting identification credentials for verification and undergoing a criminal screening/background check. Alternatively, if the vendor so chooses, it may voluntarily elect to obtain long-term credentials through enrollment, registration, background vetting, screening, issuance of credentials, and electronic validation of credentials at the vendor's own cost through a designated independent contractor NCACS service provider. Credentials will be issued every 5 years and access privileges will be reviewed and renewed on an annual basis. The costs incurred to obtain Navy installation access of any kind are not reimbursable, and the price(s) paid to obtain long-term NCACS credentials will not be approved as a direct cost of this contract. Further information regarding NCACS can be found under "Popular Links" on the CNIC Headquarters public website at http://cnic.navy.mil/CNIC_HQ_Site/index.htm."

d. Permissible Access Methods

(1) Local Passes. Vendor and contractor employees not participating in NCACS may apply for local passes subject to Federal, DoD, Department of Navy (DON), and CNIC policy and procedures for minimum screening, and subject to local

installation access rules and procedures. The local passes will be limited in duration to 1 day. See paragraph 4 of this SOP for specific procedures.

(2) CAC. Some contractors providing long-term services and requiring access to Navy information technology systems may be eligible for a CAC. Eligibility for CACs is significantly limited by law and regulation. See paragraph 5 of this SOP for specific procedures and CAC eligibility.

(3) Other Federal Credentials

(a) Validated Transportation Worker Identification Credential (TWIC) issued by the Department of Transportation is an approved DoD access card and can be used to gain access if a specific requirement to enter the installation can be verified with the appropriate documentation. TWIC shall not be accepted as a credential for unescorted physical access in and of itself. The TWIC must be accompanied by a Government or commercial bill of lading to gain access to an installation.

(b) Naval reactor identity cards issued to Naval Reactors personnel and United States Postal Service credentials are approved to access Navy installations for official business.

e. Impermissible Access Methods

(1) Uncertified commercially issued credentials and personal identification verification interoperability (PIV-I) credentials are acceptable forms of identification, but shall not be accepted as stand-alone ("flash pass") credentials for access onto any Navy installation or facility. Until such time as such credentials are determined to meet vetting standards, information assurance policies and mandates, are amenable to electronic verification, meet all legal and regulatory standards, and are officially accepted and approved by DoD, DON, and CNIC, and certified into the NCACS enterprise architectural solution, the credentials will only function as identification documents.

(2) Credentials not specified herein that have previously been or are currently produced and/or issued by Navy regions, installations, tenant commands, or other tenant organizations to vendors and contractors or other non-employees of the DON or DoD will no longer be valid for perimeter access to CNIC installations with the following exceptions identified elsewhere in this guidance:

(a) Minors (personnel under 18 years of age). See paragraph 3b(1) of this SOP for correct procedures.

(b) Vendors under the Single Source Coordinator Program. See paragraph 3 of this SOP for correct procedures.

(c) Local passes meeting the standards of this SOP. See paragraph 4 of this SOP for correct procedures.

(d) Concession food vendors and banking facility employees. See paragraph 4d of this SOP for correct procedures.

f. Sponsors. CNIC uses a methodology that involves Navy activities that "sponsor" contractors and vendors for issuance of either an NCACS credential or a CAC.

(1) NCACS Sponsoring Activities. A Navy activity that desires to sponsor a vendor company for enrollment in NCACS must be designated and approved as a Sponsoring Activity (SA) by the Approved Facility Contact (AFC), normally the force protection/physical security specialist or the Pass and Identification Office Supervisor. See paragraph 3 of this SOP for specific procedures.

(2) NCACS Single Source Coordinator (SSC). For vendors or companies having no specific relationship with a particular Navy activity, yet having a legitimate requirement for access (such as taxi, shuttle, and limousine services), the AFC may designate a Navy activity that will serve as an SSC. A typical SSC might be Navy Exchange or Fleet and Family Support Center. See paragraph 3 of this SOP for specific procedures.

(3) CAC Trusted Agents. A Navy activity that desires to sponsor a contractor employee seeking the issuance of a CAC must accomplish the application through an active duty military or civil service employee Trusted Agent (TA). TAs are approved and designated by the Trusted Agent Security Manager under the applicable procedures of the Contractor Verification System. See paragraph 5 of this SOP for specific procedures.

(4) Privilege of Sponsorship. Contractor and vendor sponsorship by SAs, SSCs, and TAs is a privilege, not a right, and the Navy reserves the discretion to remove sponsorship at any time when in the best interests of the Government.

g. Service Contractor. CNIC will accomplish the NCACS project effort utilizing contractor support ("Service Contractor").

3. NCACS Procedures

a. Enrollment. The installation and tenant organization SAs will provide the AFC a list of approved vendor and contractor companies and, for each company, the name of its designated System Company Administrator (SCA). Once the vendor or contractor company is approved, it may then enroll with the NCACS Service Contractor. For those vendor or contractor companies not included on the original approved vendor or contractor company list (ACL), the following applies:

(1) Vendor and contractor companies must be able to identify an SA of an installation/tenant activity or organization.

(2) Vendor and contractor companies must contact their SCA and send in enrollment forms to the Service Contractor, including sponsor information.

(3) The Service Contractor obtains approval or denial from the installation AFC or SA and informs the company of its status. If approved, the Service Contractor adds the vendor and contractor to the ACL.

(4) The SA may also provide the names, addresses, and associated identification information relating to vendor and contractor companies to the Service Contractor to populate the ACL in advance.

b. Registration. Once enrolled, companies may direct their employees to register into NCACS. Minors (personnel under 18 years of age) are not permitted to register in NCACS, but are authorized to receive local no-cost Navy Physical Access Control System credentials.

c. Employee Registration and Credentialing

(1) The vendor and contractor company must provide the NCACS with an approved employee list. The data required either before or during registration in NCACS may include, but is not limited to:

- (a) Name
- (b) Social security number
- (c) Company/employer information
- (d) Company address
- (e) Company phone number(s)
- (f) Contract number(s)
- (g) Contract date(s) of performance
- (h) Company-issued employee identification number
- (i) Individual digital photo
- (j) Date of birth
- (k) Fingerprints
- (l) Employee home address
- (m) Employee/personal phone numbers

(2) When the vendor or contractor employee registers into NCACS, the System Contractor conducts a background screening on each vendor or contractor employee by validating the individual's identity.

(a) Identity. To validate identity, the vendor or contractor employee must present, prior to credential issuance, one document from Appendix B, List A or B, and one document from List C. The lists of acceptable documents may be found in Form I-9, OMB No. 1115-0136, and Employee Eligibility Verification. These documents must be reviewed and deemed authentic to the satisfaction of the Government agent. The completion of the I-9 form is not required.

(3) Once the vendor or contractor employee's identity has been validated, the credential is issued. Based upon current protocols, the following procedures will apply:

(a) An NCACS credential with a green stripe will be issued to those non-CAC eligible vendors and contractors who are

United States (U.S.) citizens AND who are documented and eligible for employment in the United States. Prior to issuance of the NCACS credential, these persons will present, to the Government employee issuing the NCACS credential, a valid U.S. passport or birth certificate documenting their U.S. citizenship.

(b) An NCACS credential with a blue stripe will be issued to those non-CAC eligible vendors and contractors who are not U.S. citizens, BUT who are eligible for employment in the United States. Prior to issuance of the NCACS credential, these persons will present, to the Government employee issuing the NCACS credential, documents as required from Appendix B stating that they are eligible for employment in the United States.

(c) Non-CAC eligible vendors and contractors holding an NCACS credential with a blue or green stripe are authorized unescorted perimeter access to Navy installations covered by this policy.

(d) The credentials will be National Institute of Standards and Technology (NIST) Special Publication 800-104 Aligned Topography and a Federal Information Processing Standards (FIPS) Publication 201-1 Process Aligned.

d. Vetting/Screening Failure. If a vendor or contractor employee fails the background screening, the employee and the company are advised in writing. Reasons for failure of the background screening and denial for participation in NCACS (see Appendix C) may include, but are not limited to:

- (1) Identity verification failure
- (2) Any felony conviction
- (3) Registered sex offender
- (4) On a terrorist watch list
- (5) Any outstanding Federal, state, or local criminal warrant

e. Credential Issuance. Once NCACS participants are registered, screened, validated, approved, and credentialed by the Navy, they are then eligible to access an installation.

(1) Cleared by Service Contractor. If the vendor or contractor employee clears the background screening, the Service Contractor creates and sends the NCACS credential to the Pass and Identification Office or other designated location for issuance. The Service Contractor will inform the vendor or contractor employee of the location of the Pass and Identification Office where the credential will be issued.

(2) Navy Approval and Issuance. Subject to and in conformity with local SOPs, an approved Government employee will review and approve or deny access to the installation and issuance of the NCACS credential. At the time and place of issuance, the identity of the individual receiving the NCACS credential must be validated. The individual must present, prior to credential issuance, one document from Appendix B, List A or B, and one document from List C.

f. Validity. If the vendor or contractor employee passes the background screening process, the NCACS credential that is issued to the vendor or contractor employee is valid for up to 5 years but active for only up to 1 year at a time, with yearly fees being paid to the Service Contractor for renewals. Throughout the year, the vendor or contractor employee must continue to meet background screening standards. Periodic background screenings are conducted to verify continued NCACS participation and installation access privileges. The background screening process includes but is not limited to these occasions:

(1) When a vendor or contractor employee first registers to participate in NCACS.

(2) Periodic (every 92 days).

(3) When a vendor or contractor registers for annual NCACS renewal.

(4) At any time upon request by the Region Commander, Region Security Officer (RSO), Installation Security Officer (ISO), or the Installation Commanding Officer (CO).

g. Revocation. NCACS access privileges will be immediately suspended or revoked if at any time a vendor or contractor employee becomes ineligible. Grounds for becoming ineligible and having access privileges suspended or revoked include but are not limited to:

(1) A vendor or contractor employee no longer works for the company through which he/she enrolled.

(2) A vendor or contractor employee does not pass the background screening (initial, periodic, on annual renewal).

(3) A vendor, contractor employee, or company violates any NCACS rules, terms, or conditions.

(4) A vendor or contractor company requests that its employee be removed from NCACS.

(5) A vendor or contractor company is no longer eligible, ends its participation, or no longer does business aboard the installation.

(6) At the direction of an ISO, RSO, or CO.

h. Return of Credentials. Participating companies are required to immediately collect employee NCACS credentials. They must notify the Service Contractor or the AFC in writing if:

(1) An employee has departed the company without having properly returned or surrendered their NCACS credentials.

(2) There is a reasonable basis to conclude that an employee or former employee might pose a risk, compromise, or threat to the safety or security of the installation or anyone therein.

i. Appeals. Initial disqualification, suspension, or revocation of participation in NCACS may be appealed, as follows:

(1) Any person being denied initial participation in NCACS, or who has NCACS privileges suspended or revoked for any reason, may appeal the denial, suspension, or revocation.

(2) Vendor or contractor employees may initiate the adjudication process when a background screen failure results in disqualification from participation in NCACS and the vendor or contractor employee does not agree with the reason for disqualification. The adjudication process must be initiated within 30 days of receiving written notice of disqualification.

(3) Vendor or contractor employees may apply for a waiver when a background screening failure results in disqualification from participation in NCACS. The waiver process must be initiated within 60 days of receiving written notice of disqualification. Individuals on the Sexual Offenders Register will not be waived.

(a) All waiver requests will be initiated with a request for consideration from the ISO. The CO will be the final waiver determination authority.

(b) The ISO or CO shall consult with the installation Staff Judge Advocate when determining suitability.

j. Entry Control Point (ECP) Standards. On every ingress through a perimeter ECP, vendors or contractors participating in NCACS will present their credentials. ECP personnel will scan the credentials, which will result in the verification of the credential, and grant general access privileges and specific access profiles of time of day and day of week for that installation. ECP personnel may biometrically authenticate, using a fingerprint scan, the person presenting the credential to ensure that this is the same person who registered into NCACS. The following provides the procedures, roles, and responsibilities to successfully implement and execute the process:

(1) The participant presents NCACS credentials at the perimeter ECP to the security sentry, who will scan the credential utilizing the handheld device provided with the system.

(2) The handheld device will display a digital picture, the name of the NCACS participant, and the name of the company with which the participant is associated. This information will be checked against the local ECP server to determine if the NCACS participant has current access privileges and meets the specific access profile (day of week and time of day).

(3) If the system responds in the affirmative, and if in the opinion of the sentry the data matches the individual requesting access, AND no other mitigating safety and security factors are present, access to the installation may be granted.

(4) Generally, NCACS participants will have access to all perimeter ECPs during all hours they are open, excluding

vehicle size limitations and other physical ECP constraints. However, at credentialing, the ISO, RSO, or CO, can limit and/or assign a specific ECP to be used.

(5) Other than for Random Anti-Terrorism Measures (RAM) or in the case of an elevation of force protection conditions (FPCON), no vehicle inspection is required.

(6) If the identity of the individual requesting entry is in question, or in the case of a RAM or elevated FPCON, a biometric (fingerprint) authentication will be made to confirm that the individual is a NCACS participant.

(7) If the biometric check authenticates the individual and access privileges are current, AND no other mitigating safety and security factors are present, access to the installation may be granted.

(8) RAMs and biometric validation of the NCACS participants and their vehicles may also be conducted as deemed appropriate by the CO, RSO, or ISO.

(9) NCACS participants may not act as escorts for other persons.

(10) NCACS participants are not authorized access to restricted areas unless their NCACS credentials are authorized access and are locally required for the restricted area. NCACS participants may also be required to present a commercial or Government bill of lading when access to restricted areas is required.

(11) NCACS participants are not required to obtain and/or display DoD decals on vehicles they are operating onto an installation.

k. Interim Eligibility. Vendor or contractor employees who have registered to participate in NCACS but who have not yet completed the background screening and have not received a credential, may be provided interim access approval until they are authorized participation in NCACS or denied participation in the system.

(1) Interim access will not exceed a period of 28 calendar days.

(2) Interim access may be renewed subject to the approval of the AFC and guidance of the local SOP.

1. Taxi, Limousine, and Shuttle Access. Access procedures and standards for taxis, limousines, and shuttle services will be governed by:

(1) The NCACS as described herein;

(2) A locally issued 1-day pass (see paragraph 4 below);

or

(3) At the election of the CO, under the process and procedures of CNICINST 5530.14 CH-1. In the event that this process is made available to taxis, limousines, and shuttles, the CO must ensure compliance with all of the standards of those laws and regulations found at Appendix A of this SOP. Until these standards can be adhered to, passes will be limited in duration to one day.

4. Locally Issued Passes. In the event that a vendor or contractor elects not to participate in NCACS, or is ineligible to receive a CAC, the individual employee may apply for a locally issued pass in order to access the installation.

a. Minimum Standards. Installation procedures in issuing local passes will comply with the provisions of Federal, DoD, DON, and CNIC guidance, and will ensure at a minimum:

(1) Processing must occur at the Pass and Identification Offices under local and higher directive procedures.

(2) The vetting of personal identification information and background checks should include but is not limited to:

(a) National Criminal Investigation Check background check.

(b) The requirements set forth in OPNAVINST 1752.3, Policy for Sex Offender Tracking, Assignment, and Access Restrictions Within the Navy, of 27 May 2009, and CNICINST 1752.1, Policy for Sex Offender Tracking, Assignment, and Installation Access Restrictions, of 7 February 2011.

(c) A check against the local no entry and barment lists.

(d) Additional checks as required by current, revised, or newly issued Federal directives, DoD policy, DON policy, or CNIC directives.

(e) Additional checks as otherwise required or deemed appropriate by the RSO, ISO, or the CO.

b. Time Limitation. The CO has the authority to permit access to the installation, together with the responsibility to ensure that permitted access comports with applicable law, regulation, and policy. Accordingly, the following guidance is provided:

(1) The enterprise-wide time standard for the validity of a pass to access an installation will be not more than 1 day.

(2) If an installation identifies a need to issue passes that exceed the enterprise-wide time standard:

(a) The installation SOP will identify the basis and rationale for the time period of passes issued. Factors such as security posture, resources for monitoring, high-risk assets, and related considerations must be considered and addressed.

(b) Passes will be issued for a period of time commensurate with the level of vetting accomplished by the installation Pass and Identification Office. In the event that only minimal vetting is possible, it is anticipated that only minimal periods of access will be permitted.

(3) Periods of validity for passes may be curtailed or restricted in the future by Federal, DoD, Navy, and CNIC guidance.

c. Local SOP. As stated elsewhere in this document, installations will issue local SOPs implementing this guidance.

(1) Proposed installation SOPs will be submitted to the Region Commander for review and approval. An information copy of all installation SOPs will be furnished to CNIC Headquarters and posted to the NCACS website on CNIC's Gateway 2.0 (G2) website at:

<https://g2.cnic.navy.mil/tscnichq/N3/N3AT/SOPs/Forms/AllItems.aspx>.

(a) Unless approved at both Region and CNIC Headquarters levels, the enterprise-wide time standard for the validity of a pass to access an installation for non-NCACS participants will not exceed 1 day.

(2) The SOPs will include detailed standards and procedures for the application, issuance, and authentication of passes. Unless approved at both Region and CNIC Headquarters levels, NCACS participants will not be vetted to a greater standard than delineated in this SOP.

d. Subject to Region and Installation Commander implementation, employees of concession food vendors and banking facilities that have contracts with the Navy and have received permission to conduct business on the installation are authorized to receive local no-cost installation credentials or passes. COs and their duly delegated representatives are vested with the authority to determine eligibility and to issue cards subject to constraints of available time, resources, and competing demands of administration, operations, and missions.

(1) The issuance of any no-cost installation credential or pass is wholly discretionary, and these provisions create no right to such credentials for any vendor or any employee thereof, nor shall the Navy grant any request for reimbursement, accept any demand for equitable adjustment, or pay any claim based on failure or refusal to issue such credentials.

5. Common Access Cards

a. In most cases, general vendors or contractors are not eligible for a CAC. A CAC is not appropriate for vendor or contractor employees who provide temporary services; who merely deliver goods or supplies to Navy installations; or who are employed to provide goods or services wholly ancillary to the core Navy missions (such as workers at on-base concession stores, fast food restaurants, and snack bars). Only those individual contractors who have a legitimate basis for requesting a CAC, such as embedded (co-located) advisory and assistance contractors and contractors performing duties requiring access to Navy information technology systems (e.g., the Navy Marine Corps Intranet [NMCI]). For this purpose, eligibility to be issued a CAC will require a need for physical access to a Navy installation or facility and logical access to a Navy or DoD network (e.g., NMCI).

b. In the event a TA determines that issuance of a CAC to a specific contractor employee is appropriate, the TA must ensure that all Federal, DoD, DON, CNIC, and local rules, policies, and procedures are followed, and that proper vetting and background investigations are accomplished. The TA is responsible for compliance with the following authorities:

(1) Directive Type Memorandum (DTM) 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance" dated 1 DEC 2008, updated 10 August 2010;

(2) Directive Type Memorandum (DTM) 08-006, "DoD Implementation of Homeland Security Presidential Directive - 12 (HSPD-12)" dated 26 November 2008, updated 10 August 2010;

(3) Federal Information Processing Standards (FIPS) Publication 201-1;

(4) Office of Management and Budget (OMB) M-05-24, dated 5 August 2005; and

(5) Contractor Verification System administered by the Defense Manpower Data Center.

6. Responsibilities

a. The vendor or contractor company is solely responsible for enrollment and registration into NCACS.

b. Installations are responsible to:

(1) Issue written guidance and implement local SOPs that articulate the specific provisions and requirements of the project. These SOPs may be supplemented by installations to the extent that they do not conflict or give authority beyond the guidelines established in the SOP, Federal law, and DoD or DON policy. All activity supplements must be approved by the parent Navy Region.

(2) COs have the authority over, and responsibility for, the safety and security of an installation. While discretion is vested in the authority of the CO, compliance with all legal requirements must be adhered to, and deviation from the guidance of this SOP must be subject to careful consideration.

(3) Identify an AFC. Responsibilities may include, but are not limited to, providing an ACL, identifying the NCACS sponsor(s), coordinating command, installation, and tenant sponsor briefings, coordinating guard/police training, and developing SOPs for implementation of NCACS installation access.

(4) Monitor the NCACS ECP servers and registration stations being supported with communications and power requirements. Ensure the NCACS is provided with the required space, electrical power, and dedicated communication lines required by the Service Contractor for the program to be operational. Conduct routine operational and corrective action procedures for system functionality.

c. Tenant organizations will provide an ACL, identify NCACS sponsor(s), and ensure updates to both.

d. The NCACS Service Contractor is responsible to:

(1) Purchase and maintain ownership of system hardware and software.

(2) Install equipment.

(3) Coordinate implementation of NCACS.

(4) Communicate with vendors and contractors participating in NCACS.

(5) Conduct a background screening(s) on the participating vendors or contractor employees.

(6) Manufacture a Federal/Navy-approved format credential if the vendor or contractor employee passes the background screening.

(7) Forward and submit all manufactured credentials to the Navy AFC for approval and issuance.

(8) Notify vendor or contractor employees that their NCACS credentials have been forwarded to the Navy for issuance. Inform the vendor or contractor employees of the location of the Navy Visitor Control Center where the credentials will be issued.

(9) Monitor access privileges, which will be immediately suspended or revoked if at any time a vendor or contractor employee becomes ineligible to continue participation in NCACS.

(10) Provide monthly reporting on the NCACS System to the installation.

(11) Provide life cycle maintenance and support for the NCACS.

Appendix A

List of Applicable Authorities

- HSPD-12, Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors
- Directive Type Memorandum (DTM), DTM-09-12, Interim Policy Guidance for DoD Physical Access Control
- FIPS-201, Federal Information Processing Standards, Personal Identity Verification of Federal Employees and Contractors
- Public Law 110-181 (FY 2008) Section 1069, Standards for Entry to Military Installations in the United States
- OPNAVINST 1752.3, Policy for Sex Offender Tracking, Assignment, and Access Restrictions Within the Navy
- CNICINST 1752.1, Policy for Sex Offender Tracking, Assignment, and Installation Access Restrictions
- DTM 08-003, Next Generation Common Access Card (CAC) Implementation Guide, September 27, 2011
- OPNAVINST 5530.14E Navy Physical Security and Law Enforcement Program, April 10, 2010
- CNICINST 5530.14 CH-1, CNIC Ashore Protection Program

Appendix B

LISTS OF ACCEPTABLE DOCUMENTS

All documents must be unexpired

LIST A Documents that Establish Both Identity and Employment Authorization	OR	LIST B Documents that Establish Identity	AND	LIST C Documents that Establish Employment Authorization
1. U.S. Passport or U.S. Passport Card		1. Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address		1. Social Security Account Number card other than one that specifies on the face that the issuance of the card does not authorize employment in the United States
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)				2. Certification of Birth Abroad issued by the Department of State (Form FS-545)
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa		2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address		3. Certification of Report of Birth issued by the Department of State (Form DS-1350)
4. Employment Authorization Document that contains a photograph (Form I-766)		3. School ID card with a photograph		4. Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
5. In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing 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		4. Voter's registration card		5. Native American tribal document
		5. U.S. Military card or draft record		
		6. Military dependent's ID card		6. U.S. Citizen ID Card (Form I-197)
		7. U.S. Coast Guard Merchant Mariner Card		
		8. Native American tribal document		
6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI		9. Driver's license issued by a Canadian government authority		7. Identification Card for Use of Resident Citizen in the United States (Form I-179)
		For persons under age 18 who are unable to present a document listed above:		
		10. School record or report card		
		11. Clinic, doctor, or hospital record		
		12. Day-care or nursery school record		8. Employment authorization document issued by the Department of Homeland Security

Illustrations of many of these documents appear in Part 8 of the Handbook for Employers (M-274)

Appendix C

NCACS Prototype Vetting Sources and Government Watch Lists

- NCACS background screens are conducted through a third-party background check provider.
- Background screens include but are not limited to:
 - SSN trace
 - Address verification and 10-year address history
 - National Criminal Database (NCD)
 - NCD contains 250+ million records, including data from all 50 states and all available state-wide criminal databases
 - 50-state electronic scan and development of a county criminal search
 - County criminal search
 - Review of county court records
 - National Federal criminal search
 - Review of all Federal criminal courts
 - Nationwide sexual offender database
 - 50-state, District of Columbia, Guam, and Puerto Rico review of all sexual offender registries
 - Terrorist screen
 - Office of Foreign Assets Control (OFAC) list for known terrorist associates
 - Outstanding criminal wants/warrants: felonies and misdemeanors
 - Comprehensive background scans are conducted annually
 - Electronic background screens are conducted every 92 days
 - Waiver and adjudication processes are in place
- Other government watch lists
 - U.S. Department of Commerce Denied Person's List
 - Fugitive List (compiled from FBI, U.S. Marshal, and U.S. Secret Service Most Wanted Lists and Drug Enforcement Administration (DEA) Fugitive List)
 - Interpol Most Wanted List
 - Office of Thrift Supervision List
 - Australian Reserve Bank Sanctions List
 - Bank of England Sanctions List
 - National Security Debarred Parties List
 - Directorate of Defense Trade Controls
 - European Union Terrorism Sanctions List

CNICNOTE 5530
5 Jul 2012

- o Food and Drug Administration (FDA) Office of
Regulatory Affairs Debarment List