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

CANC: 25 APR 12
CNICNOTE 5530
N3

CNIC NOTICE 5530

From: Commander, Navy Installations Command

Subj: IMPLEMENTATION OF NAVY COMMERCIAL ACCESS CONTROL SYSTEM WITHIN CONUS REGIONS, NAVY REGION HAWAII AND JOINT REGION MARIANAS

Ref: (a) OPNAVINST 5530.14E
(b) DTM 09-12 Directive Type Memorandum
(c) HSDP-12 Homeland Security Presidential Directive
(d) FIPS 201 Federal Information Processing

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

1. Purpose. To document Navy Commercial Access Control System (NCACS) as the current reference term that replaces the "RAPIDGATE" Program and to implement the NCACS Project for Navy Regions in the Continental United States (CONUS), Navy Region Hawaii and Joint Region Marianas.

2. Background

a. References (a),(b),(c) and (d) provides over-arching Navy policy, guidance, information, procedures and responsibilities for the Navy Physical Security and Law Enforcement Program. The NCACS is an operational application of Navy security and law enforcement policy. It operates on the principle of driver, rather than cargo, verification 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 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. Other than for Random Anti-Terrorism Measures (RAM) or in the case of an elevation of Force Protection Conditions (FPCON), no commercial vehicle inspection is required.

(2) A credential is issued and base access 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 (NCIC).

(3) The process of vetting, the maintenance of databases, the creation of credentials, and the technology required for authentication will be provided by a service contractor under the NCACS.

(4) Installation/Regional 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.

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

(6) Costs to vendor participants are recaptured through increased productivity of their employees due to the reduction of wait time at the Pass and Identification Offices and at entry control points.

3. Policy

a. Implementation of NCACS shall:

(1) 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 Common Access Card (CAC).

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

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

(4) Comply with best security practices and Defense Information Assurance Certification and Accreditation Process (DIACAP) information assurance (IA) controls and prohibits the storage of Personally Identifiable Information (PII) on mobile devices.

(5) Ensure electronic perimeter installation access control management in near real time by individuals and company. Privileges are granted by time of day, day of week and by installation. Privileges of non-CAC vendors/contractors may be extended to more than one installation if authorized.

4. Responsibilities

a. Each Region will be responsible for establishing a NCACS point of contact (POC) providing the individuals contact information to CNIC N61 via email to Sharon.gibson@navy.mil.

b. Each Region will ensure that each installation will comply with the 5530 NCACS Notice/SOP and that each Installation will be responsible for establishing a NCACS Standard Operating Procedure (SOP) and Post Orders. Enclosure (1), CNIC NCACS SOP, contains the minimum mandatory requirements for NCACS implementation.

c. Installations will be responsible for maintaining a one-day Visitor Pass program for those non-CAC vendors/contractors who choose not to enroll in the NCACS.

(1) Installations will be responsible for ensuring, as per local implementing SOPs, that Visitor Passes are issued in compliance with Federal, DoD, DON and CNIC guidance.

(2) Local commanders are responsible for determining what level of future resourcing is required for Pass and Identification Offices in the event that NCACS results in reducing the demands upon such offices.

5. Program Support

a. As stated above, NCACS program performance and administration will be accomplished through a service contractor.

b. The current service contractor is Eid Passport, Incorporated, Portland, Oregon.

c. Eid Passport, Incorporated, will utilize the *RAPID*Gate system to accomplish vetting, credentialing, and authentication.

d. In the event that new or additional service contractors are selected to administer NCACS, notice will be provided.

6. Forms and Reports. The NCACS produces 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.

7. Nomenclature. Previous designations of the NCACS have included "*RAPID*Gate" and "Non-Common Access Card Credentialing for Vendors/Contractors" (NC3VC) Program, and "Navy Quick Credentials" (NQC) Project. All references to previous names and titles of the NCACS Project are to be updated and corrected to conform to current usage.

M. C. Vitale

M. C. VITALE
Vice Admiral, U.S. Navy

Distribution:
Electronic only, via CNIC Gateway 2.0

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 (ECPs) equipped with the Navy Commercial Access Control System (NCACS).

2. Background.

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

b. Objective and Goals. Implementation of 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/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/contractors, their vehicles and throughput of all vehicles coming aboard CNIC installations.

c. Voluntary. Participation in NCACS is not mandatory. This SOP does not eliminate other traditional methods of permitting access to Navy Installations such as local passes, CAC, and other approved federal credentials.

d. Permissible Access Methods.

(1) Local Passes. Vendor/contractor employees not participating in NCACS may apply for local passes subject to Federal, DoD, DON and CNIC policy and procedures for minimum screening, and local installation access rules and procedures. The local passes will be limited in duration to one (1) day. See Paragraph 4 of this Standard Operating Procedure (SOP) for specifics.

(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. 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 the installation can be verified through documentation. Under most circumstances, the TWIC must be accompanied by a Government or Commercial Bill of Lading.

e. Impermissible Access Methods.

(1) PIV-I. Personal Identification Verification Interoperability (PIV-I) credentials are not generally accepted as access "flash pass" documents and do not comport with required standards of vetting. See Appendix A. Until such time as a PIV-I is determined to meet vetting standards, be amenable to electronic verification, meet all legal and regulatory standards, and is officially accepted and approved by DoD, DON and CNIC, the credential will be limited to an identification document.

(2) Credentials (not specified herein), that have previously or are currently produced and/or issued by Navy regions, installations, Navy tenant commands and/or other tenant organizations to vendors/contractors or other non-employees of the Department of the Navy or the Department of Defense will no longer be valid for perimeter access to CNIC installations.

f. Sponsors. CNIC uses a methodology that involves Navy activities that "sponsor" contractors and vendors for issuance of either a 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. For vendors/contractors 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 a Single Source Coordinator (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 (TASM) under the applicable procedures of the Contractor Verification System (CVS). See Paragraph 5 of this SOP for specific procedures and CAC eligibility.

(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. Implementation. CNIC issued Notice 5530 and companion SOP to provide clear direction on implementation of NCACS. NCACS is being implemented by Navy Region in two (2) phases.

(1) Phase 1: Enrollment/Registration, Vetting, and Credentialing (NCACS Credential used as a "flash pass"). This component is anticipated to be fully implemented across the CNIC enterprise no later than 29 July 2011.

(a) At each installation, Phase 1 will be implemented and the requirements of CNIC Notice 5530 and SOP enclosure adopted within 12 to 16 weeks after the ICO receives the NCACS Installation Command Brief.

(2) Phase 2: Electronic Enforcement. This component is anticipated to be fully implemented across the CNIC enterprise no later than 31 October 2011.

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

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

(2) Vendor/contractor companies must contact System Company and send in enrollment forms to the Service Contractor including sponsor information.

(3) Service Contractor obtains approval or denial from the Installation AFC or SA and informs the company of their status. If approved, the Service Contractor adds the Vendor/Contractor into the ACL.

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

c. Registration. Once enrolled, those companies may direct their employees to register into NCACS.

d. Employee Registration and Credentialing.

(1) The vendor/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/contractor employee(s) registers into NCACS, the Service Contractor conducts a background screening on each vendor/contractor employee by validating an individual's identity and biometrically authenticating their enrollment into the system.

(a) Identity. To validate identity, the vendor/contractor employee must present prior to credential issuance one document from Appendix B, List A or if unavailable, two documents from Appendix B, List B. 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.

(b) Biometrics. To biometrically authenticate enrollment into the system, the credential will be scanned and the fingerprint biometric captured utilizing the handheld device provided with the system.

(3) Once the vendor/contractor employee's identity has been validated and enrollment into the system biometrically authenticated, the credential is issued.

(a) The credentials will be NIST-Special Publication 800-104 Aligned Topography and FIPS PUB 201-1 Process Aligned.

e. Vetting/Screening Failure. If a vendor/contractor employee fails the background screening, the employee and their company are advised in writing. Reasons for failure of the

background screening and denial for participation in NCACS, see Appendix A, 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

f. Credential Issuance. Once a NCACS participant is registered, screened, validated, approved and credentialed by the Navy, they are now eligible to access an installation.

(1) Cleared By Service Contractor. If the vendor/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/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 the 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 if unavailable, two documents from Appendix B, List B.

g. Validity. If the vendor/contractor employee passes the background screening process, the NCACS credential that is issued to the vendor/contractor employee is valid for up to one year. Throughout the year the vendor/contractor employee must continue to meet background screening standards. Periodic background screenings are conducted to verify continued NCACS participation and installation access privileges. Background screening includes, but is not limited to:

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

(2) Periodic (every 92 days).

(3) When vendor/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 (ICO).

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

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

(2) A vendor/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/contractor company requests their employee be removed from NCACS.

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

(6) At the direction of an ISO/RSO/ICO.

i. Return of Credentials. Participating companies are required to immediately collect employee NCACS credentials and notify the Service Contractor or the AFC in writing:

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

(2) That 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.

j. Appeals. Appealing initial disqualification, suspension or revocation of participation in NCACS.

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

(2) Vendor/contractor employees may initiate the adjudication process when a background screen failure results in disqualification from participation in NCACS and the vendor/contractor employees 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/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. Members on the Sexual Offenders Register will not be waived.

(a) All waiver requests will be initiated with the ISO. The ICO will be the final waiver determination authority.

(b) The ISO/ICO shall consult with the Installation Staff Judge Advocate when determining suitability.

k. Entry Control Point (ECP) Standards. On every ingress through a perimeter ECP, vendors/contractors participating in NCACS will present their credential. ECP personnel will scan the credential which will result in the verification of the credential, and grant of general access privileges and specific access profiles (time of day, 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 System:

(1) The participant presents their 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 company name with whom 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 ICO, 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 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 ICO, RSO, or ISO.

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

(10) NCACS participants are not authorized access to restricted areas unless they have their NCACS credential and are authorized access (and as locally required) for the restricted area. NCACS participants may also be required to present a Commercial Bill of Lading 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.

1. Interim Eligibility. Vendor/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 twenty-eight (28) calendar days.

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

m. 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 one (1) day pass (Paragraph 4 below); or

(3) At the election of the ICO, under the process and procedures outlined in CNICINST 5530.1A. In the event this process is made available to taxis, limousines and shuttles, the ICO must ensure compliance with all of the standards of those laws and regulations found at Appendix B 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/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 to the installation.

a. Minimum Standards. Installations procedures in issuing local passes will comport with the provisions of Federal, DOD, Navy, 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 Crime Information Center (NCIC) 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 ICO.

b. Time Limitation. The ICO 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 one (1) day.

(2) If an ICO 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 Visitor Control Center/Pass Office. In the event that only minimal vetting is possible, it is to be 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 Regional Commander for review and approval. An information copy of all Installation SOPs will be furnished to Headquarters CNIC.

(a) Unless approved at both Regional 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 one (1) day.

(2) The SOPs will include detailed standards and

procedures for the application, issuance, and the authentication of passes.

(a) Unless approved at both Regional and CNIC Headquarters levels, NCACS participants will not be vetted to a greater standard than delineated in this SOP.

5. Common Access Cards.

a. In most cases, general vendors/contractors are not eligible for a CAC. A CAC is not appropriate for vendor/contractor employees who provide temporary services; who are hired for short-term (less than six months); 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 an on-base concession store/snack bar). Only those individual contractors who have a legitimate basis for requesting a CAC, such as embedded (co-located) advisory and assistance contractors; contractors having long-term and routine access to multiple installations to support core Navy functions; contractors performing duties requiring access to Navy Information Technology systems (e.g., the Navy Marine Corps Internet [NMCI]); and contractors performing under Statements of Work (SOWs) and Performance Work Statements that properly and legitimately identify their personnel as qualified for a CAC will be considered eligible. For this purpose, entitlement to a CAC will require a need for both physical access to a Navy installation or facility AND logical access to 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 investigation(s) are accomplished. The TA is responsible for compliance with the following authorities:

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

(2) Directive Type Memorandum 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 Publication 201-1;

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

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

6. Responsibilities

a. Enrollment and registration into NCACS is the sole responsibility of the vendor/contractor company.

b. Installations will issue written guidance, implementing local SOPs that articulate the specific provisions and requirements of the project. This SOP may be supplemented by Installations to the extent that it does not conflict or give authority beyond the guidelines established in the SOP, federal law and DoD/DON policy. All Installation supplements must be approved by the parent Navy Region.

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

d. Installations will identify an Approved Facility Contact (AFC). Responsibilities may include, but are not limited to, providing an Approved Company List (ACL), identifying the NCACS sponsor(s), coordinating command, installation and tenant sponsor briefings, coordinate guard/police training, development of SOPs for implementation of NCACS installation access.

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

f. 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/contractors participating in NCACS.

(5) Conduct a background screening(s) on the participating vendor/contractor employee(s).

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

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

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

(9) Monitor access privileges which will be immediately suspended or revoked, if at any time a vendor/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

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 Statewide criminal databases
        - 50-state electronic scan and a 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 associations
    - 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, US Marshal and US Secret Service Most Wanted Lists and the 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
    - FDA Office of Regulatory Affairs Debarment List

- OFSI (Canadian Sanctions List)
- United Nations Consolidated Sanctions List
- Palestinian Legislative Council List
- U.S. General Services Administration Excluded Parties List
- World Bank Listing of Ineligible Individuals
- Note: Specific Watch Lists that are included in the background screening may vary from time to time.

Appendix B

List of Applicable Authorities

- HSPD-12, Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors
- DTM-09-12, Directive Type Memorandum, 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

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. Voter's registration card		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		5. U.S. Military card or draft record		
		6. Military dependent's ID card		
		7. U.S. Coast Guard Merchant Mariner Card		5. Native American tribal document
		8. Native American tribal document		6. U.S. Citizen ID Card (Form I-197)
		9. Driver's license issued by a Canadian government authority		
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		**For persons under age 18 who are unable to present a document listed above:**		7. Identification Card for Use of Resident Citizen in the United States (Form I-179)
		10. School record or report card		8. Employment authorization document issued by the Department of Homeland Security
		11. Clinic, doctor, or hospital record		
		12. Day-care or nursery school record		

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