



Department of the Navy

Common Access Card Sustainment Plan

FY04 through FY06

**June 24, 2004
Version 1.4**

I. INTRODUCTION	3
II. SUSTAINMENT AND MAINTENANCE TASKS	5
III. CAC SUSTAINMENT APPROACH	6
IV. RISK AND RISK MITIGATION	8
V. RESOURCES AND FUNDING	9
VI. VII. REFERENCES	10
APPENDIX A: ACRONYM DEFINITION TABLE	11
APPENDIX B: CAC MAINTENANCE PLAN	13
APPENDIX C: CAC RE-ISSUANCE PLAN SUPPLEMENTAL	17
APPENDIX D: CONSOLIDATED PASS & ID OFFICE INITIATIVE	21

I.

Introduction

A. Purpose & Overview

The purpose of the Department of the Navy (DON) Common Access Card (CAC) Sustainment Plan is to coordinate activities to transition from initial mass issuance of the CAC to steady state sustained CAC issuance and maintenance operations.

Initial mass issuance of the CAC focused on meeting the Department of Defense (DoD) CAC initial issuance mandate and supporting the fielding of the Navy Marine Corps Intranet (NMCI). Permanent Real-time Automated Personal Identification System (RAPIDS) sites and augmentation using temporary CAC issuance workstations accomplished initial issuance. This augmentation, called mass issuance, helped reduce the initial issuance workload on permanent CAC RAPIDS issuance sites. The expense of continuing the use of temporary CAC issuance workstations is considered prohibitive and will end in FY04.

Sustained CAC issuance and maintenance will be transitioned from the eBusiness Operations Office (eBUSOPSOFF) to the Commander Navy Installations (CNI) for ashore RAPIDS workstations and Commander Fleet Forces Command (CFFC) for afloat RAPIDS workstations.

Sustained CAC operations will include:

1. Initial issuance to new personnel; and
2. CAC maintenance to reset a CAC personal identification number (PIN) or update data on the CAC integrated circuit chip (ICC); and
3. Re-issuance due to expiration, technology failure (chip, magnetic stripe, 3 of 9 barcode and PDF 417 barcode), operational replacement (rank change, name change, privilege change and expiration) and/or other reasons to replace a CAC, damaged, lost/stolen, confiscated and PKI compromised cards.

This overview and summary document addresses plans for issuance/re-issuance, maintenance and actions to consolidate CAC sustainment operations with other base operations support activities to improve customer service and reduce cost.

B. Background and Situational Assessment

DoD Directive 8190.3 currently sets the policy for the Smart Card Technology and establishes the CAC as the DoD smart card. Defense Manpower Data Center (DMDC) is responsible for fielding and sustaining the DEERS/RAPIDS infrastructure to issue and sustain the CAC. The Defense Information Systems Agency (DISA) is responsible for fielding and sustaining the the DoD Public Key Infrastructure (PKI) certificate generation system that is integrated with the DEERS/RAPIDS infrastructure. PKI information is encoded on the Integrated Circuit Chip (ICC) when the CAC is issued from a RAPIDS workstation.

The RAPIDS workstation also encodes the ICC with a user selected PIN. The user must remember the PIN to allow computer applications to access data on the ICC. If after three attempts a user does not respond to a PIN request with

their correct PIN the CAC ICC is locked and must be reset before future use. Currently the PIN on a locked CAC may only be reset at a RAPIDS workstation. Planning is ongoing by CNI for the installation of CAC PIN Reset (CPR) workstations to assist with changing or unlocking PINs on the local level.

The initial DMDC support concept for the CAC proposed:

1. A web based portal, User Maintenance Portal/Post Issuance Portal (UMP/PIP) that would allow a cardholder to update their CAC ICC from their desktop computer. Planned ICC updates included:
 - a. PKI certificate updates
 - b. Smart card applets download & removal
 - c. PIN reset
2. A Central Issuance Facility (CIF) that would process a locally generated request for a CAC, print the CAC at a central location using a high-speed printer and mail it to the recipient. The CIF would support initial issuance at high volume sites like the Service Academies, recruit sites, basic military training schools, and users at remote sites, like Embassies, overseas locations and reserve site, where a very few individuals needed to be issued a CAC and a RAPIDS workstation was unavailable. Eventually, the CIF will also support re-issuance of the CAC to all personnel.

At this time these support capabilities are not available to meet near term CAC sustainment and maintenance requirements. The only tool to issue and update a CAC is a RAPIDS workstation. RAPIDS workstations are permanently installed at Customer Support Desks (CSD), Personnel Support Activity Detachments (PSDs) and at some installation Pass & ID/Tag Offices. Additionally, the temporary RAPIDS workstations used for mass issuance by the DON eBUSOPSOFF are also available through FY-04 to help meet emerging CAC sustainment and maintenance requirements.

C. CAC Sustainment and Maintenance Requirements

The fielding of NMCI capabilities that use the PKI certificates on the CAC presents the largest maintenance requirement the CAC Sustainment Plan must address. Lessons learned shows approximately 75% of CAC holders do not recall the PIN they selected when their CAC was issued if not used regularly within the first 30 days. This requires individuals to get their PIN reset. Additionally, a majority of CAC holders need to have the PKI certificates updated to enable the ability to utilize cryptographic logon (CLO) and encrypt/digitally sign email using NMCI email address.

The CAC re-issuance "bow wave" represents the second requirement to be addressed by the Sustainment Plan. In 2001, the eBUSOPSOFF began supplementing initial CAC issuance using temporary RAPIDS workstations at many installations. Beginning in 2004, a large CAC re-issuance requirement is anticipated at these early mass issuance sites due to the fact most CACs expire three years after issuance. During FY-04 some temporary RAPIDS workstation are available to supplement installations with a large re-issuance workload. Due to the prohibitive costs associated with this supplemental issuance, this type of augmentation will not be available in FY-05 and beyond. Permanent RAPIDS sites must be able to support their CAC re-issuance requirements beyond FY-04.

Efforts to place additional RAPIDS workstations at specific locations to meet these requirements are in progress.

D. CAC Sustainment and Maintenance Stakeholders

DMDC operates and maintains the DEERS/RAPIDS infrastructure. They are developing the CIF for CAC issuance and the UMP/PIP to maintain the CAC.

DISA operates and maintains the PKI Certificate Authority Servers and infrastructure that interfaces with the DEERS/RAPIDS infrastructure.

DON CIO is the Information Technology (IT) oversight authority to the United States Navy (USN) and United States Marine Corps (USMC).

DON eBUSOPSOFF is the facilitator of the transition of CAC sustainment and maintenance activities to CNI by 1 October 2004.

CNO N614 is the CAC program coordinator within the USN.

CFFC manages and provides oversight of the afloat CAC operations.

CNI manages and provides oversight of the ashore CAC operations.

PERSCOM-67 is the RAPIDS Project Officer for the USN.

NETWARCOM is responsible for overseeing implementation of PKI within the Navy, PKI for the Fleets, including tracking the issuance of CACs distributed to Fleet personnel.

NMCI Program Management Office directs and manages actions related to EDS fielding and supporting the NMCI infrastructure, enabling the CAC for cryptographic login, digital signatures and email encryption.

HQMC C4 is the program sponsor for PKI activities and CAC issuance within the USMC.

HQMC M&RA is the RAPIDS Project Officer for the USMC.

Region Command Leadership primary focus is to support the sustainment and use of the CAC via policy acceptance, communication, and mobilizing personnel for CAC updates.

II. Sustainment and Maintenance Tasks

A. Initial CAC Issuance

DoD policy required all eligible DoD personnel to have a CAC by 1 April 2004. Initial issuance after this date should be limited to new military accessions and newly hired civilians and contractors.

B. CAC Maintenance

CAC maintenance tasks are those actions that change information on the CAC ICC after issuance. The most common CAC maintenance tasks are CPR and PKI certificate update (i.e. ID, email encryption and digital signing certificates), which are currently done at RAPIDS workstations. However, CAC maintenance also includes updating the ICC with the download of the JDM, which currently requires a RAPIDS workstation. CAC maintenance for use with other smart card applications (i.e. Card Maintenance Utility and Food Service) can be completed using a properly configured standard computer.

C. Re-issuance of CACs

CACs are re-issued when:

1. The CAC expires
2. A technology failure occurs (chip, magnetic stripe, 3 of 9 barcode and PDF 417 barcode)
3. An operational replacement is required (rank change, name change, privilege change and expiration)
4. Other reasons to replace the CAC are realized (damaged, lost/stolen, confiscated and PK compromised)

To manage the large number of cards expected to expire during FY-04, 05 and 06, an approach must be developed to stagger subsequent expirations and augment current permanent RAPIDS and other available resources.

III. CAC Sustainment Approach

A. Initial Issuance Approach

Under long-term strategic sustainment conditions, new military accessions will get their CAC from the CIF when it becomes available. CACs issued to these individuals will have only the PKI ID certificate and the JDM written to the ICC. The CAC will be updated with the other PKI certificates when the sailor has an initial requirement to access a Navy network or needs the JDM applet for smart card applications. Until the CIF is operational new Navy military recruits will receive their CAC at the Navy's Recruit Training Center at Great Lakes from RAPIDS workstations. Marine Corps recruits will not be issued a CAC during recruit training, but will get their first CAC when they report to their first assignment or get their first promotion.

New Navy and Marine Corps civilians and contractors are issued their first CAC at the installation where they are employed.

Until the CIF is operational the only source to issue or re-issue a CAC is a RAPIDS workstation at a CSD, PSD or Pass & ID/Tag Office.

B. Maintenance Approach

The driving reasons for CAC maintenance are the fielding of PKI functionality and smart card applications that use the CAC.

CAC Maintenance in support of PKI Functionality

The two most common systems that use PKI are NMCI and the Defense Travel System (DTS).

The NMCI Program Management Office (PMO) will incrementally provide PKI functionality as they upgrade over 100 NMCI server farms supporting NMCI users.

For an NMCI user to be able to use the PKI functionality of their NMCI workstation (logon and digital signing or encrypting of emails) they must have a fully functional CAC where:

- The user knows his/her PIN
- Three PKI certificates were encoded to the ICC – ID certificate, digital signature certificate, and digital encryption certificate.
- The ICC has PKI email certificates issued after May 18, 2002
- The ICC has PKI email certificates issued using their NMCI email address

If any of these conditions are not met the NMCI user must revisit a RAPIDS workstation to have their CAC updated (CAC PINs may be reset from a CPR workstation when they become available).

For a DTS user to be able to use their CAC with the DTS system they must know their PIN.

The approach for CAC maintenance in support of NMCI and DTS is to provide **ALL** CAC maintenance needs during one visit to a RAPIDS site, as soon as a site or organization is notified of either DTS fielding or NMCI PKI implementation. The goal of this “one-touch” service in a just-in-time method is to make the CAC maintenance experience as convenient as possible and accomplish it as close as possible to the time when a fully functional CAC is needed.

CAC Maintenance in support of smart card applications

The CNI CAC PMO is completing plans for the Navy-wide implementation of the Card Maintenance Utility and Food Service smart card applications. Use of these applications require the JDM applet be downloaded (instantiated) on the user’s current CAC. JDM applet download currently requires a RAPIDS workstation, and therefore CAC maintenance will be integrated with initial deployment of the smart card applications if deemed necessary. Augmentation of CAC maintenance will be determined on a case by case basis after considering all aspects of deploying the smart card application and existing CAC maintenance capability at the installation.

[Refer to Appendix B: CAC Maintenance Plan for more details.](#)

C. Re-issuance Approach

At some Navy locations, mass issuance of CAC cards will result in a “bow-waves” of card re-issuance three years after the initial mass issuance. Navy installations with large civil servant populations and where a mass issuance occurred are most likely to experience this renewal “bow-wave”. Installations where the population is primarily military or contractor or where there was no mass issuance will not likely be impacted as CACs expire. The challenge is to project how many CACs will expire and when they will expire. Using this

information and historical dependent and retiree ID card issuance information, the local PSD and Pass & ID Offices can assess their re-issuance workload and if necessary take proactive measures to manage it.

The eBusiness Operations Office will make available projected CAC expiration information sorted by Navy Installation and PERS-673 will make available historical ID card issuance statistics. Officers in Charge at the PSD and Pass & ID Office should use this information to plan how they will locally manage their projected workload for their base/installation.

[Refer to Appendix C: CAC Re-issuance Plan for more details.](#)

IV. Risk and Risk Mitigation

Risk: Customer inconvenience and alienation

Mitigation Plan: Focus on “one touch” customer support and convenience of CAC maintenance service, use of web-based appointment scheduling. The plan will not be implemented until NMCI PMO demonstrates full PKI functionality.

Risk: Capacity to handle the issuance and maintenance using only permanent RAPIDS workstations.

Mitigation Plan: Identify locations for workstation and/or operator augmentation

Risk: CAC users forgetting their PINs after being reset

Mitigation Plan: Develop a Just-in-Time approach and have the RAPIDS operator stress the importance of remembering the PIN and suggest ways to choose a PIN.

Risk: Low customer turnout for CAC maintenance

Mitigation Plan: Senior level support of CAC maintenance, good Public Affairs Office (PAO) campaign, and use of web-based appointment scheduling

Risk: Coordination of NMCI server farm upgrades and CAC maintenance activity

Mitigation Plan: Close communication of NMCI server farm upgrades and lessons learned from CAC maintenance, clear timeline established for NMCI PKI implementation.

Risk: Availability of DMDC proposed CIF or web-based CAC maintenance tools

Mitigation Plan: Use RAPIDS terminals until the CAC maintenance capabilities are operational

Risk: Availability of CAC issuance infrastructure

Mitigation Plan: Use the web-based scheduler to notify customers when system is slow or unavailable

Risk: Permanent RAPIDS site awareness of re-issuance guidelines

Mitigation Plan: Policy message and updates from PERS-673 to all RAPIDS sites.

V. Resources and Funding

A. Consolidation of CAC Sustainment and Maintenance Resources

With the CSD, PSD and Pass & ID/Tag Offices now under the oversight of the CNI, the opportunity to consolidate CAC issuance facilities exists. This consolidation opportunity has the potential to provide improved customer service while reducing overall cost of these presently disparate operations. To assess the value of consolidating these CAC issuance and base access facilities, Personnel Support Activity (PSA) Atlantic in conjunction CNI, the eBUSOPSOFF and the Mid-Atlantic Region will operate a consolidated CAC issuance and base access facility at a location within the Mid Atlantic Region. The purpose of the initiative will be to determine the benefits from consolidating functions from the CSD, PSD and Pass & ID/Tag Offices and provide a benefit analysis to Navy resource managers. This initiative is called the Consolidated Pass and ID Office (CPIDO).

[Refer to Appendix D: Consolidated Pass & ID Office Initiative for more details.](#)

B. Required RAPIDS infrastructure for sustained operations

To achieve the goals of the sustainment approach within this plan, a heavy reliance will be placed on the RAPIDS infrastructure and CAC issuance web based applications (web scheduler, the temporary RAPIDS CAC Application for Statistics and TimeTrade initiative under development) as they become available. During the initial period of PKI and smart card implementation, CAC maintenance and CAC sustainment for initial issue expirations, augmentation to both the permanent RAPIDS workstations and operators may be provided by the eBUSOPSOFF during FY04 for a high-intensity, short duration (i.e. two weeks) operational period.

For long-term sustained operations, a determination of required infrastructure will be made by PERS-673 and adjustments made by the eBUSOPSOFF during FY04 implemented accordingly. To determine the CAC issuance sustainment requirement, the following formula will be used (1 RAPIDS workstation averages 30 CACs per 8 hour day (no CAC maintenance is in these figures):

$$\frac{\text{CAC Re-issuance Requirement}^{****}}{X^{**}} + \text{Historical Teslin Issuance}^* = \frac{30^{***}}{1}$$

*All Teslin activities including Joint Services

** Number of RAPIDS Workstations required

*** Ration of number of actions to workstation per day

**** CAC Re-issuance Requirement to include the historical percentage of DoD cross servicing

Currently the Web Scheduler and the temporary RAPIDS CAC Application for Statistics are available to manage scheduling and issuance. These applications will transition to CNI for hosting and management. Other long-term web tools are in development by DMDC for allowing users to update and manage PKI certificates and PINs.

VI. VII. References

- A. Department of Defense Directive 4630.5 Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
- B. Department of Defense Directive 8190.3, Smart Card Technology
- C. Department of Defense Directive 8500.1 Information Assurance (IA)
- D. Department of Defense Directive 8500.1 Information Assurance (IA) Implementation
- E. OUSD (P&R)/DODCIO memo of 16 Jan 01, Common Access Card (CAC)
- F. OUSD (P&R)/DODCIO memo of 18 Apr 02, Common Access Card (CAC) - Changes
- G. DODCIO memo of 12 Aug 00, Department of Defense (DoD) Public Key Infrastructure (PKI)
- H. DOD CIO memo of 17 May 01, Public Key Enabling (PKE) of Applications, Web Servers, and Networks in the Department of Defense (DOD)
- I. ASD (C3I) memo of 21 May 02, Public Key Infrastructure (PKI) Policy Update
- J. SECNAV WASHINGTON DC 301903Z Mar 01, Common Access Card
- K. DONCIO memo of 19 May 03, Smart Card and Public Key Infrastructure (PKI) policy
- L. DOD Instruction 1000.13, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals
- M. BUPERS Instruction 1750.10B, Identification (ID) Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Personnel
- N. Real-Time Automated Personnel Identification System (RAPIDS) Verifying Official (VO) Certificate Practice Statement of 12 Sep 01
- O. RAPIDS Training Guide (v.6) with Addendum dated Apr 01
- P. CNO WASHINGTON DC 221800Z FEB 01, Procedures for Issuing the Common Access Card (CAC)
- Q. COMNAVPERSCOM MILLINGTON TN 261200Z APR 01, Implementation of the Common Access Card (CAC)
- R. COMNAVPERSCOM MILLINGTON TN 261526Z NOV 01, Common Access Card (CAC) Issuance Procedures
- S. COMNAVPERSCOM MILLINGTON TN 161852Z SEP 02, Common Access Card (CAC) and ID Card Updates

Appendix A: Acronym Definition Table

ACRONYM	DEFINITION
ASD	Assistant Secretary of Defense
BUMED	Bureau of Medicine & Surgery (US Navy)
BUPERS	Bureau of Naval Personnel
CAC	Common Access Card
CFFC	Commander Fleet Forces Command
CIF	Central Issuance Facility
CIO	Chief Information Officer
CLO	Cryptographic Logon
CNO	Chief of Naval Operations
CPR	CAC PIN Reset
CNI	Commander Navy Installations
COR	Contractor Officer's Representative
COTR	Contractor Officer's Technical Representative
CSD	Customer Support Desk
CVS	Contractor Verification System
CY	Calendar Year
DEERS	Defense Eligibility Enrollment Reporting System
DISA	Defense Information Systems Agency (US DoD)
DMDC	Defense Management Data Center
DoD	Department of Defense
DON	Department of the Navy
eBUSOPSOFF	eBusiness Operations Office
FY	Fiscal Year
HQMC	Headquarters, Marine Corps
ICC	Integrated Circuit Chip
ID	Identification
IT	Information Technology
JDM	Joint Data Model
LAN	Local Area Network
M&RA	Manpower & Reserve Affairs
NETWARCOM	Naval Network Warfare Command
NMCI	Navy Marine Corps Intranet
OCONUS	Outside the Continental United States
OUSD	Office of the Under Secretary of Defense
PAO	Public Affairs Officer
PERSCOM	Personnel Command
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMO	Program Management Office
POC	Point of Contact
PSA	Personnel Support Activity
PSD	Personnel Support Activity Detachment
RAPIDS	Real-Time Automated Personnel Identification System

SSM	Site Security Manager
SSN	Social Security Number
TA	Trusted Agent
UMP/PIP	User Maintenance Portal / Post Issuance Portal
USN	United States Navy
USMC	United States Marine Corps
WAN	Wide Area Network

Appendix B: CAC Maintenance Plan

I. INTRODUCTION

A. Purpose & Overview

The purpose of the Common Access Card (CAC) Maintenance Supplement is to coordinate activities that provide DON personnel with a fully functional CAC to take advantage of information assurance functions and smart card applications.

This section of the overall DON Sustainment Plan provides specific information and details that supplements the plan's first five sections

B. Background and Situational Assessment

In 2002, the CAC infrastructure experienced problems handling the large demand placed upon it. This resulted in poor system availability, longer times to issue or update a CAC and long lines at RAPIDS sites. For the most part, the problems with the CAC infrastructure have been corrected; however, many people remember these difficult times and are reluctant to visit a RAPIDS site to get their CAC issued or updated. Additionally, many CACs were issued without the required PKI certificates. This will cause the holder to get their CAC updated before using any system that uses the CAC.

The long-term CAC support concept is to update information on the CAC Integrated Circuit Chip (ICC) from a web-based application. It is envisioned that an individual will be able to change their email signing and encryption PKI certificates, download the smart card Joint Data Model (JDM) applet, or reset the CAC PIN from a desktop computer. This capability is not available at this time.

To support the CAC PIN reset function, the Army funded DMDC to develop a CAC PIN Reset (CPR) workstation that uses a dial-up or Ethernet connection to individually reset PINs. CNI is in the process of acquiring and planning the implementation of 50 CPR workstations.

A User Maintenance Portal/Post Issuance Portal (UMP/PIP) is being developed by DMDC to support the updating of email PKI certificates and downloading the smart card JDM applet. While it is targeted to have UMP/PIP available for late FY04, initial functionality will only include email certificate updates. Fielding plans for the UMP/PIP have not been determined as of the publish date of this document. To find the latest information regarding UMP/PIP, go to DMDC's website at <http://www.dmdc.osd.mil> and click on the "What's New" link.

II. CAC Maintenance Requirements

CAC Maintenance requirements are distinct for three separate population types, those individuals who are or will be accessing the NMCI Network, those who will be accessing other non-NMCI DON networks such as the Bureau of Medicine & Surgery (US Navy) (BUMED) and Outside the Continental United States (OCONUS) locations, and those who will use smart card applications.

A. NMCI Users

Initial fielding of NMCI workstations did not include full PKI functionality. Full PKI functionality will sequentially be implemented at NMCI server farms supporting specific geographical areas and DON installations. Determining the NMCI CAC maintenance requirements presents some challenges due to the following circumstances:

- The number of NMCI users who have forgotten the CAC PIN is unknown
- The number of NMCI users with PKI email certificates issued on or before May 19, 2002 is unknown
- The number of NMCI users with PKI email certificates issued with a non-NMCI email address is unknown
- NMCI users who are not cutover do not know their NMCI email address prior to getting their CAC updated
- Implementation of full PKI functionality at server farms is still in planning
- All NMCI users at a DON installation may not be provided full PKI capability at the same time

As a result of the above circumstances, NMCI CAC maintenance requirements will vary from installation to installation. At each installation the approach to CAC maintenance must be coordinated locally between the NMCI local Customer Service Representative and the RAPIDS site OICs to ensure NMCI CAC maintenance needs are met prior to PKI enablement of NMCI workstations. It is important that the number of NMCI users transitioning to PKI does not saturate with the NMCI Help Desk or capacity of the installation's RAPIDS workstations. The rate and sequencing of NMCI workstation transition will be a government decision lead by the NMCI Customer Service Representative for the installation.

B. Non-NMCI Network Users

Requirements to maintain the CAC by users who access non-NMCI networks will depend on when and how CLO, email encryption and digital signatures are implemented on their specific network. Current evaluation indicates that the work needed to support the CAC will primarily be CAC PIN resets and minimal email certificate updates.

C. Smart Card Application Users

CAC maintenance in support of fielding smart card applications using the JDM consists of:

1. Instantiating a CAC with the JDM
2. Writing data to the JDM applet (the space set aside to hold data on the CAC ICC)

Once the JDM is instantiated through the download from a RAPIDS workstation, data is written to the ICC using a Card Maintenance Utility workstation. To use a JDM smart card application a CAC holder must:

- Know their CAC PIN
- Have a CAC with the JDM instantiated on the ICC (Food Service, Manifest Tracking and Weapons Issuance do not require the JDM, but make the smart card applications more efficient if there is a correctly populated JDM on the CAC).
- Have the data used by the JDM smart card application encoded on the ICC

Every person who will use a JDM smart card application will require CAC maintenance.

III. CAC Maintenance Approach

The DON CAC Maintenance approach is to provide customers with “one-touch, just-In-time” service prior to when the PKI/CAC enabled network functions are made available. In order to reduce the number of times a customer needs to visit a RAPIDS sites and spread out the future expiration of CACs, RAPIDS sites are encouraged to consider integrating CAC maintenance actions and re-issuance actions whenever it makes sense.

A. NMCI Network Users

The NMCI program office plans a phased approach to implementing PKI. The goal is to provide PKI capability to NMCI users at the time they are cutover to NMCI. However there are some NMCI users that have already been cutover that do not have PKI capability. Their local NMCI Customer Service Representative will notify these NMCI users when they will need to use their CAC to perform PKI functions. They should get CAC maintenance performed prior to that time.

B. Non-NMCI Network Users

Specific implementation plans for CAC maintenance for non-NMCI networks will be developed in conjunction with the implementation of email encryption, digital signatures, and CLO.

C. Smart Card Application CAC maintenance

For most DON CAC application users, CAC maintenance will be integrated with initial deployment of the smart card application. This will normally require CAC maintenance augmentation from the eBUSOPSOFF through the use of temporary RAPIDS workstations available in FY04. Augmentation will be determined in a case-by-case basis after considering all aspects of deploying the CAC application and existing CAC maintenance capability at the installation.

VI. Resources and Funding

A. RAPIDS workstations

Temporary workstations will be augmented by the DON eBUSOPSOFF through the end of FY04. These workstations will be used to fill a short-term need of doing initial card maintenance and re-issuance, which will smooth the re-issuance cycle demand during FY05 and FY06. Due to the limited number of workstations available, these will be assigned on a requirement basis. In FY05, some temporary workstations may be converted to UMP/PIP or CPR machines and provided to CNI for distribution.

B. UMP/PIP

DMDC’s UMP/PIP workstations are the desired long-term maintenance tool. This application-based tool will be available in the future, but are not available at this time.

C. CPR

The CPR workstations will be used as an augmentation tool for resetting individual user’s CAC PIN. Policy and resource management will be a function of the CNI Deputy CIO’s office as a function of CNI’s centralization of CAC and PKI support services. Initial procurement of fifty (50) workstations will be funded by SPAWAR with CNI to develop a distribution plan to the individual Region staffs. This application-based tool will be available in the future, but are not available at this time.

D. Personnel augmentation

Temporary personnel must be vetted and trained prior to operating a RAPIDS workstation. The DON eBUSOPSOFF, through the end of FY04, may be able to provide qualified temporary support personnel, if, by evaluation, it proves to be a cost effective mean of CAC maintenance and re-issuance support for a short duration.

Appendix C: CAC Re-issuance Plan

I. General Information

A. Purpose

This section of the document provides an approach to manage CAC re-issuance so it can be accomplished within existing resources with minimal impact to personnel and the operational mission.

B. Re-issuance Approach

CAC re-issuance is a responsibility of the commands and organizations with permanently installed RAPIDS workstations and falls under the direct management and oversight of the local command structure – activity, base, station, installation, or Region. Re-issuance must be managed locally; however this plan provides a structured approach to help local management accomplish re-issuance.

C. The Re-issuance Population

The population involved in planning CAC re-issuance may be segregated into three distinct categories.

1. Military. All active duty personnel and member of the Selected Reserve. CAC re-issuance for the military category of personnel will generally be completed in conjunction with specific events:
 - a. reenlistment,
 - b. promotion/advancement,
 - c. contract extension,
 - d. name change,
 - e. privilege change,
 - f. damaged or lost/stolen card,
 - g. technology failure on the card
 - h. and expiration

These events are considered normal and therefore do not require mass re-issuance planning. Military CAC re-issuance will take place at the servicing CSD and PSD. CAC re-issuance scheduling concurrent with the completion of administrative requirements for these events/activities can be facilitated by use of the web-based appointment scheduler. Use of this tool is available to all permanent RAPIDS card issuance sites and has a proven track record for regulating the workload on the RAPIDS facilities.

2. DoD Federal Civil Servants. All DoD federal civil servants require a CAC regardless of occupational series or grade. Because of the inherent stability (lack of turnover or geographic relocation) of this population, DoD civil servants are the primary focus for re-issuance planning.
3. Authorized DoD Contractors. All DoD contractors requiring a CAC for physical access to an installation/building or for logical access to DoD communications or computing systems (which requires a PKI Class III token) are eligible to be issued a CAC. CAC expiration is generally associated with the expiration date of the applicable contractor contract. Because contract termination dates are

usually spread across the fiscal year, planning for large scale CAC replacement/re-issuance is usually not required. However in those cases where contracts involving large numbers of support contractors will expire during a short timeframe, CAC issuance/re-issuance may be better managed using the web-based appointment scheduler. In the future the Contractor Verification System (CVS), the automated system by which DoD contractors apply, and are approved or disapproved for issuance of a CAC, will also be available to streamline re-issuance to the contractor population. Use of the web-scheduler and CVS will preclude time lost by contractors waiting for CAC re-issuance when compared to a first-come, first-served process frequently employed at CAC issuance offices.

[See Attachment A for contractor responsibilities that should be included in all contracts.](#)

D. Re-issuance Planning

CAC re-issuance is a command level responsibility and must be implemented and coordinated across all functional areas. The DON eBusiness Operations Office will provide estimates of expected CAC expirations and PERS-673 would provide historical ID card issuance statistics so local RAPIDS site leadership can plan to accommodate their re-issuance requirements.

Local base, station, installation, and/or Region staff involvement is required to assure CAC re-issuance success. Delay in planning and implementation of re-issuance will lead to an unacceptably large bow-wave re-issuance requirement, which can only be satisfied locally by extending the hours of operation of sustainment sites. The following steps are recommended to assure early planning and successful CAC re-issuance:

- Participate in and support planning and coordination meetings.
- Identify a point of contact (POC) to serve as centralized coordinator if re-issuance activities.
- Develop formal CAC re-issuance plan – prioritize personnel requiring CAC re-issuance.
- Use the web-based appointment scheduler to assist in managing re-issuance workflow, while minimizing lost time/time off-task for employees.
- Manage and aggressively implement a local communications/public affairs announcements/ awareness campaign. Proactively remind current cardholders of the need for replacement, and the documentation required.
- Provide all necessary connectivity to the local area network (LAN) or wide area network (WAN)
- Provide issuance schedule for activities (and personnel, if desired).
- Provide any needed transportation of target population to sustainment issuance locations, if applicable.
- Assist coordinating local personnel to man re-issuance workstations if needed
- Provide all necessary physical security for the re-issuance equipment
- Identify government officials who are authorized to sign a contractor's DD 1172-2 or act as a Trusted Agent (TA) using the Contractor Verification System (CVS) and provide a list of those officials to the CAC re-issuance sites on the installation.
- Assist in entering authorized contractor's data and CAC request form DD 1172-2 into DEERS.

Re-issuance should primarily focus on DON civil servants since they comprise the most stable re-issuance population and can be supported by an effective re-issuance plan. All DON federal civil servants should be directed to schedule a CAC re-issuance appointment during their individual birth months. Use of the web-based appointment scheduler is strongly recommended to manage the workload and to avoid protracted local delays due to site overloading.

Re-issuance of Military member CACs should be tied to personnel actions and contractor CAC re-issuance will be managed using the web based scheduling application and CVS system IAW the proposed contract clause. See Attachment A.

D. Re-issuance Support

Augmentation for re-issuance will be available until the start of FY-05. Beyond FY-04 the DON eBusiness Operations Office is not funded to support issue or re-issue of the CAC. In FY-04 the DON eBusiness Operations Office will focus augmenting re-issuance at those sites that have a significant DOD civil servant population or had initial mass issuance in 2001. Re-issuance will be coordinated with NMCI transition to PKI if possible. Beginning in FY-05 re-issuance workload will fall directly on the local RAPIDS sites.

Attachment A - Contract Clause for all Support Contracts

Key points needing to be captured:

- CACs are controlled government issued identification cards. As such, each CAC issued, lost, replaced or revoked must be accounted for.
- Contractors are responsible for requesting the issuance of a CAC to one of their employees based on physical and logical access requirements of each contract employee.
- Contractors will submit the DoD CAC DEERS Enrollment Form (DD Form 1172-2) requests for CACs to the Contracting Officer's Representative/ Contracting Officer Technical Representative (COR/COTR).
- When it becomes available contractors will use the CVS to request a CAC for a contract employee whenever possible.
- Contractors are required to notify the COR/COTR when a contract employee no longer needs a CAC to perform the tasks in the contract or the contract employee is no longer performing tasks under the contract
- Contractors are responsible for recovering CAC's issued to a contract employee when the CAC is no longer needed.
- Contractors are required to return recovered CACs via registered mail to the local issuance site.

Appendix D: Consolidated Pass & ID Office Initiative

I. Introduction

A. Purpose & Overview

The Consolidated Pass & ID Office (CPIDO) Initiative presents the Department of the Navy (DON) the opportunity to explore opportunities to obtain cost benefits, efficiencies, and Quality of Life (QOL) improvements by implementing a centralized office for issuing all organizational identification cards and passes. The scope of the initiative is to implement a limited range of revised business rules and processes at a specific installation location and documenting additional improvements to be made. The end-term result will be the development of an Opportunity Analysis with enterprise implementation recommendations. Upon initiative implementation, the first set of data for analysis will be available for review after 60 days, with additional data available every 30 days for a total of 180 days.

The initiative will assess the adaptability of a new business model that combines similar functions performed at disparate locations for different customer categories. Consolidated id card and pass issuance should improve the quality of customer service, reduce customer's lost work hours, prove the value of scheduled service, and permit optimized use of resources consumed in the Pass & ID issuance process. Measurable statistics will be kept for number of pass or ID card issued, issuance times, cost of operation, resource utilization, and customer satisfaction.

B. Background and Situational Assessment

ID card and installation pass issuance within the DON is reflective of business practices and procedures pre-dating the advent of the Defense Eligibility Enrollment Reporting System (DEERS)/Real-time Automated Personnel Identification System (RAPIDS) system. Today, issuance sites are generally associated with the categories of customer serviced rather than the type of service provided. Issuance site locations generally do not reflect the changing population demographics associated with the fielding of the Common Access Card (CAC) and operation changes associated with that fielding.

The current distribution of RAPIDS workstations is influenced by organizational roles, is not reflective of optimal business practices, and is redundant in both space allocation and personnel requirements. The initiative goal is to centralize issuance of all ID cards, privilege cards, access control badges, and physical installation passes (i.e. vehicle stickers) for all personnel categories, including DOD-mandated cross servicing, at single site for the selected installation.

C. Initiative Scope

The CPIDO will operate under the authority of the Regional Commander and direction and management of his/her designee(s). The mission of the CPIDO is to centralize issuance of all ID cards, local physical access control cards, and vehicle passes for the designated initiative location. For the purposes of the initiative, Navy-owned temporary DEERS/RAPIDS workstations and temporary contractor personnel may be employed.

The customer-base for the initiative office is all individuals (i.e. government service, military, retirees, family members, and contractors) who need access to the installation and require some type of identification card and/or vehicle pass. By providing these

customers a single site with easy access outside the base parameter, the office will provide better, more reliable customer service, consolidate resources, and improve installation security posture. Initiative scope will be narrow in nature as to the category of services provide. Those services will be limited to functions currently provided by the NAVSTA Norfolk PSD and Pass & ID offices. Additional expansion to other services maybe recommended in the Opportunity Analysis document, to be written at the end of the initiative.

II. Initiative Objectives

The initiative will examine the value of centralized operation using an activity based costing model. Assessable elements of the initiative include cost of facility upgrades, staffing, operational infrastructure support, and consumable inventory. A project management plan will be created prior to the start of the initiative, identifying key milestone, tasks and task owners, schedules, and expected resource requirements. This plan will be updated and reviewed regularly throughout the 180 days of the initiative by the CPIDO Initiative Working Group.

The initiative will conduct a complete examination of various options for operation and identify the most balanced method based cost efficiency and operational effectiveness. Components in determining efficiency of cost include scope of required work; work hours, customer flow, and staffing levels. Operational effectiveness will include customer wait times, number of individual transactions, number of multiple transactions for an individual, and patron satisfaction levels.

The objectives and functional responsibilities of the initiative are:

1. Centrally locate the issuance of all installation ID cards, access badges, and vehicle decals.
2. Utilization of currently available tools to schedule and manage customer appointments
3. Incorporate the Contractor Verification System (CVS) for automated Form DD 1172-2 processing for contractor personnel needing a Common Access Card (CAC).
4. Leverage current and future technologies to streamline the process of issuing and maintaining personal identification cards and access control devices such as vehicle decals and building badges.
5. Reduce lost customer work hours (wait times) and "walk-in" business by scheduling appointments
6. Provide CAC maintenance support for NMCI, PKI capability, and JDM applications.
7. Determine the appropriate manning mix through workload analysis

III. Expected Results

1. Recommendation to reduce the number of badge/ID issuance sites from the present average of two per installation to one.
2. Recommendation to reallocate manpower requirements at PSDs and Pass & ID Offices through staff integration.
3. Recommendation to create a centralized installation access control database to partially automate support of base access control of vehicles and buildings.
4. Recommendation to provide the ability for commands and installations to have real-time visitor control information.

Recommendation to establish a regional vehicle decal system vice issuance of individual base decals, such as used at CNRMA, in all USN Regions.

IV. Initiative Methodology

The initiative will be conducted in four phases; planning, design and development, implementation, and assessment.

Initiative Planning Components

- Identification of physical location
- Obtaining Regional Commander consent and cooperation
- Development of detailed concept of operations
- Pre-initiative metric data gathering
- Current operational business analysis
- Development of future business operation processes, policies and procedures
- Development of initiative budget
- Development of initiative schedule
- Development of initiative work breakdown structure (WBS)
- Development of PAO/Communication Plan
- Development of Initiative Transition Plan

Site design and development Components

- **Physical site design**
- **Office outfitting planning and implementation**
- **Customer Notification Campaign**
- **Determine staffing responsibilities and conduct cross training of personnel**
- **Implementation of new business processes, policies, and procedures**

Operational Implementation and Review

- **Provide key functionality to clients**
- **Collect metrics as needed for evaluation**

Initiative Assessment

- Business Opportunity Analysis
- Lessons Learned
- Recommended Standard Operating Procedures (SOP)
- Implementation Plan
- **Tools Recommendation Document**

V. Initiative Stakeholders

DMDC operates and maintains the DEERS/RAPIDS infrastructure. .

CNI manages and provides oversight of the ashore operations and enterprise installation policies.

DON eBUSOPSOFF is the facilitator of the CPIDO initiative, providing oversight and project management.

PERS-33 is the military manpower organization and RAPIDS Project Officer for the USN.

Office of Civilian Human Resources is the civilian manpower organization for the DON.

Regional Commander is responsible for overseeing the implementation of the initial initiative in following the DON eBusiness Office Initiative plan.

PSA/PSD & Regional Security are responsible for developing and implementing CPIDO business processes and gathering data to access initiative effectiveness.

VI. Initiative Success Criteria

Project success is measurable and quantifiable in terms of:

- ID cards issuance throughput
- Issuance time
- Customer wait time
- Customer satisfaction
- Required physical space
- Required staffing levels
- Required training by function in hours
- Cost benefit analysis of new operational procedures
- True cost of business or activity by operational category

Additionally, the initiative will be successfully concluded when the following documents are developed:

- Business Opportunity Analysis
- Lessons Learned
- Recommended Standard Operating Procedures (SOP)
- Implementation Plan
- Tools Recommendation Document

VII. Risk and Risk Mitigation

Risk: Customer inconvenience and alienation

Mitigation Plan: Create a PAO campaign to inform customer base of changes and new service location, scheduling procedures, and operational hours.

Risk: Transition from current business processes to new business processes without degradation service.

Mitigation Plan: Have redundant capability and overlap service until new processes are proven successful.

Risk: Insufficient capacity to handle the issuance and maintenance using current permanent RAPIDS workstations.

Mitigation Plan: Focus on workstation and operator augmentation if needed

Risk: Lack of Regional leadership awareness and support.

Mitigation Plan: Brief the Regional Board of Directors to the goals, duration and anticipated advances created by the initiative.

Risk: An existing critical function, currently in place today, will be overlooked and not provided for adequately.

Mitigation Plan: All operational departments and divisions will be requested to participate in the review of proposed business processes.

VIII. Resources and Funding

A. RAPIDS workstations

The DON eBUSOPSOFF through the end the initiative or FY04, whichever comes first, will augment temporary RAPIDS workstations. These workstations will be used to fill a short-term need of conducting the initiative. Do to the limited number of workstations available; these will be assigned on a requirement basis.

B. Personnel

Manning for the CPIDO will be established by reassigning existing PSD and Pass & Tag employees. The opportunity to supplement with contractors will be based on the requirement as determined by workload analysis. This analysis will be the baseline for recommendations concerning the organization structure at enterprise implementation. Responsibility for the positions is at the Regional Commander level and funded through CNI. The DON eBusiness Office will augment, if needed, temporary personnel.

C. Facilities

The Regional Commander will provide the facility for the CPIDO. Needed upgrades or modifications will be identified and requested by the CPIDO Initiative Working Group. The Regional Commander will approve all modifications. The DON eBusiness Office will fund essential facility upgrades and acquisition of temporary facilities.