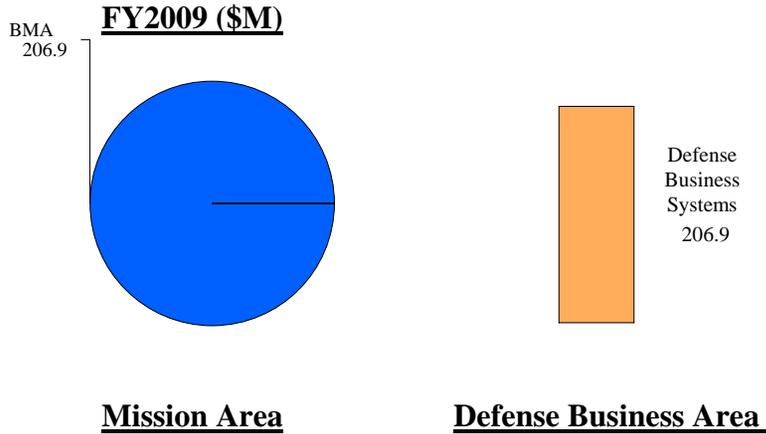


**Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008**



FY08/09PB Comparison (\$M)

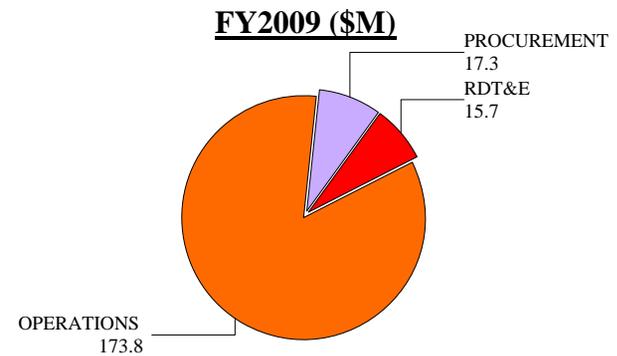
	<u>FY2007</u>	<u>FY2008</u>	<u>FY2009</u>
PB FY2008:	\$ 137.1	\$ 116.3	\$ 163.6
PB FY2009:	\$ 141.3	\$ 133.1	\$ 206.9
Delta:	\$ 4.3	\$ 16.8	\$ 43.3

Explain:
Refer to 'Significant Changes' section of the Overview

FY08 to FY09 Comparison (\$M)

	<u>FY2008</u>	<u>FY2009</u>	<u>Delta</u>
PB FY2009:	\$ 133.1	\$ 206.9	\$ 73.8

Explain:
Refer to 'Significant Changes' section of the Overview



APPROPRIATION

**Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008**

Page left intentionally blank

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

Executive Summary

The Defense Human Resources Activity's Information Technology Budget supports the Field Activity's mission to provide exceptional and innovative support, information management, and administrative services to the DoD components on human resource matters and to collect, archive and provide management information, research and analysis of human resources and other related functional area databases throughout the Department. DHRA's programs and associated systems result in improved service, performance, and satisfaction for users throughout the Department. DHRA's major IT efforts include the Defense Eligibility Enrollment Reporting System (DEERS) and the Defense Civilian Personnel Data System (DCPDS), the Department's enterprise HR information and automated processing system that supports over 800,000 employee records. These programs play an essential role in achieving the government-wide goals associated with the President's Management Agenda.

Significant Changes

The delta between the FY 2008 and FY 2009 funding lines reflects an increase in funding for the Defense Enrollment Eligibility Reporting System (DEERS) for hardware upgrades and software improvements; an increase in funding for Real Time Automated Personnel Identification System (RAPIDS) for hardware and software technology refresh to include new FIPS standards for HSPD-12, partially offset by reduced funding for the Common Access Card (CAC) due to partial funding of the baseline program for FY 2008.

The FY 2009 budget reflects increased operational requirements and planning initiatives, including funds for the initial consolidation of DCPDS regional server operations and the initial conceptual design of a potential integrated HR/Payroll automated system. In FY 2009 RDT&E funds of \$15.7M, \$9.3M procurement and \$2.2M O&M funds (\$27.2M total) support initial DCPDS server consolidation and conceptual design for potential integrated HR/Payroll.

The delta from FY 2008 to FY 2009 also reflects resources to support an HR/payroll prototype aimed at proof-of-concept for supporting potential integration of civilian payroll data, processing, and reporting capability into DCPDS. Funding increases also reflect the start-up funding for the consolidation of DCPDS regional operations to a single site for more efficient regional DCPDS operations formerly operated by the DCPDS Component customers. The technical architecture will be upgraded beginning in FY 2009 to support continued migration of DCPDS regional databases to a consolidated architecture. Additionally, in FY 2009 CPMS will deploy a critical enterprise staffing solution to support the civilian staffing and recruitment processes. Funds are also provided in FY 2009 for DCPDS sustainment activities to support NSPS and automation of SES performance management.

Procurement funds are for DCPDS lifecycle replacement and upgrades of hardware and software. The system functions in a standard operating environment of servers, workstations, and peripherals, using open systems-complaint hardware and software platforms with standard communications protocols over the Defense Information System Network (DISN). In FY 2009 DCPDS start-up for consolidation of regional server operation to a single site will initiate more efficient operations previously operated by Component customers.

RTD&E funds in FY 2009 support an HR/payroll prototype for supporting potential integration of payroll data, processing, and reporting into DCPDS.

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

Defense Business Systems

Both DEERS/RAPIDS/CAC and DCPDS are business systems and have been certified by the Human Resources Management (HRM) Investment Review Board (IRB) for the expenditure of funds in FY 08, and approved by the Defense Business Systems Management Committee (DBSMC), in accordance with 10 U.S.C. §2222.

DEERS/RAPIDS/CAC:

DEERS is the Department-wide, Joint Service, fully operational central personal data repository containing personnel data on over 35 million individuals with employment or benefit relationships with the DoD. This system interfaces with the Real-time Automated Personnel Identification System (RAPIDS) and the Common Access Card (CAC) systems. These systems collectively provide transformational technology that allows compliance with cutting edge security requirements and legislative mandates affecting the entire federal sector. Mission critical functions support Benefits Delivery, Homeland Security, and Personnel and Readiness.

In September, 2006 and again in September 2007, DEERS was approved for additional funding by the Human Resources Management (HRM) Investment Review Board (IRB) for activities related to compliance with the Homeland Security Presidential Directive 12 (HSPD-12). With the additional funding for HSPD-12 compliance activities, DEERS will:

- Meet the mandatory requirements of the Presidential Directive.
- Integrate with FBI and Defense biometric identification systems to provide real time authentication against criminal and terrorist watch lists.
- Track changes in personnel status and aid in criminal investigations.
- Verify visitor identity/authorization.
- Provide security personnel notices on persons of interest attempting to access facilities and increased personnel protection and policy compliance.
- Restrict access of people that do not have a requirement to be in DoD infrastructure, either physically or logically.

DCPDS:

DCPDS is identified as a mission essential information system, based on the Defense Information Technology Portfolio Repository (DITPR) and carries a Mission Assurance Category (MAC) II. DCPDS software development/implementation is critical to the National Security Personnel System (NSPS) and is on the critical path for NSPS implementation. The modernization actions to support NSPS were reviewed by the Human Resources Management Investment Review Board recommended for certification and were approved by the DBSMC.

NSPS is a flexible and contemporary civilian personnel management system that contains new business rules for how civilians are hired, assigned, compensated, promoted, and disciplined, within the framework of merit principles. NSPS has required updates and modifications to the existing Defense Civilian Personnel Data System (DCPDS) business rules, interfaces and reports to accommodate new rules, regulations, and processes based on the design of NSPS, such as pay banding, pay for performance, new Reduction-In-Force (RIF) rules, new appointing authorities, and new kinds of personnel transactions, including conversion in and out. Further changes to DCPDS to support NSPS will continue in FY 2009.

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

Information Assurance Activities

DEERS/RAPIDS/CAC:

DEERS underwent extensive security review in FY2005. This included both a review by the National Security Agency (NSA) as part of the implementation of the Common Access Card (CAC) as well as a separate Certification and Accreditation (C&A). This was completed in May of 2005 and resulted in an Authority to Operate (ATO) granted by the DEERS Designated Approving Authority (DAA). This process incorporates testing for compliance of security controls as specified in DODD 8500.2, OMB-A130 and the National Institute for Standards and Technology (NIST) Security Handbook. DEERS maintains compliance with the annual Federal Information Security Management Act (FISMA) review process. DEERS has an up-to-date security plan (System Security Authorization Agreement in accordance with DITSCAP (DoDI 5200.40 and DoD 8510.1-M)), meeting DoD, FISMA, OMB policy and NIST guidelines. The security plan is part of the C&A, which occurs every three years, but is supplemented by an update twice a year; it includes scans for vulnerabilities and the creation of a Plan of Action and Milestones to remediate and append to the overall security plan. In addition, as audits occur, their comments and remediation of their recommendations also become part of the security plan. DMDC underwent a successful Basic Survivability Assessment (BSA) by the Defense Threat Reduction Agency. Rather than being a technical assessment, it was an Operational Security assessment (OPSEC). This type of assessment attempts to identify organizational and procedural weaknesses from the perspective of an adversary, and then make recommendations to ameliorate the weaknesses. In addition, in FY07, DEERS conducted a successful test of its Contingency Plan. Methods have been developed for training systems users including Security Awareness Training for employees and contractors prior to their receipt of an authorized network account on the network. Specialized in-house security training provides security expertise to different functional areas (UNIX and/or WINDOWS, System Administrators and more). DEERS deployed intrusion detection devices and countermeasures around the logical perimeter of DEERS data holdings. The DEERS local and wide-area networks were certified and accredited by independent auditors to operate at Mission Assurance Category (MAC) level 2, sensitive. DEERS also implemented many of the recommendations stemming from 2 NSA audits and 1 DTRA survivability audit, thereby further enhancing network security. In FY08, DEERS will undergo a full C&A process to include the new DIACAP standards in addition to the annual FISMA compliance activities and updating of the System Security Plan and Contingency Plan testing. In FY07, DEERS completed a Privacy Impact Assessment (PIA) and published the results on http://www.dmdc.osd.mil/documents/PIA_DEERS.pdf. Further, the System of Record Notice was republished on its new hosted website at <http://www.defenselink.mil/privacy/notices/osd/dmdc02.html>.

DCPDS:

DCPDS has the authority to operate as of February 22, 2000. A complete re-accreditation of DCPDS was completed during FY 2008. The DAA re-accredited the system on November 8, 2007, in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). DCPDS is being converted to the DoD Information Assurance Certification and Accreditation Process (DIACAP), with full accreditation under DIACAP complete in spring 2008. In FY 2008 completion of CAC-enabled DCPDS, accompanied by Reduced Sign-On, is on schedule. A service level agreement with Army Research Lab was initiated to support CNDSF service for DCPDS.

Sensitive personal data is protected by:

- Physical security with site certifications
- Enclave boundary protection
- Network
- Application

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

- Data Security
- Specific user roles and responsibilities
- Encryption and cryptography
- Data protection in storage and in transit
- Personnel Security
- Continuous IA training for users, managers, employees, and contractors
- Defense-in-depth, balancing protection with cost, performance, and operational considerations
- Continuous systems monitoring and establishment of Hewlett Packard OpenView (HPOV) operations center

Major Accomplishments

Both the DEERS and DCPDS programs have made significant accomplishments supporting improved delivery of services, expanded capabilities, improved operations, incorporation of new technologies, and achievement of set goals supporting medical, security, and personnel communities throughout the Department. Efforts support the strategic plans and goals of the Department, the Office of the Under Secretary of Defense for Personnel and Readiness, and the President's Management Agenda.

DEERS/RAPIDS/CAC:

Defense Enrollment Eligibility Reporting System (DEERS), Real Time Automated Personnel Identification System (RAPIDS), and the Common Access Card (CAC). The DEERS, RAPIDS, and CAC programs are inter-related and inter-dependent operational systems that promote an efficient flow of business processes. DEERS is the Department of Defense's (DoD) person data repository (PDR) of all personnel and certain health care enrollment and benefit eligibility data. CAC uses the DEERS database for authentication and personnel information. RAPIDS is the infrastructure that supports the Uniformed Services identification card, provides on-line updates to DEERS and issues the CAC to Service members, civilian employees, and eligible contractors, thus providing an enterprise-wide credential for both physical and logical access to DoD facilities and networks.

DEERS is the central DoD repository of all personnel and certain health care enrollment and benefit eligibility data. DEERS houses data on over 35 million people for identity purposes and ensures only eligible beneficiaries receive benefits and entitlements. These include medical, dental, pharmacy, commissary and exchange privileges, life insurance and educational benefits ((e.g. Montgomery GI Bill (MGIB), Reserve Educational Assistance Program (REAP), National Call to Service)). DEERS collects and maintains demographic data on eligible beneficiaries, improving the planning, allocation and management of DoD benefits, ensuring that taxpayer dollars are used for the purposes intended by Congress and the President.

Critical to the transformation of the DoD MHS. DEERS provides over 35 applications and 40 interfaces to hundreds of military healthcare systems. The design of DEERS has allowed DoD to add enterprise solutions quickly and efficiently. This results in better, more cost effective service to the members and the war fighters. Leveraging the infrastructure has proven benefits: first, the time to develop and field is extremely short; second, the information is consistent and uniformly available anywhere in the DoD; and third, the expense to the DoD of building another stovepipe system is avoided. Value-added benefits include:

- Database of record for eligibility, enrollments, fees and catastrophic cap/deductibles, improving customer care, and reducing potential fraud while improving data quality
- Portability of health care information, reducing reliance on paper-based files that can be lost or misplaced when service members and other eligible beneficiaries relocate
- Central repository of Other Health Insurance information to improve third party collections resulting in savings for the Military Healthcare System

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

- Support “One TRICARE” mindset, even if administered by multiple organizations, providing a consistent look to our beneficiaries by enforcing standardized processes, producing consistent correspondence, providing a common enrollment application and common applications for customer service
- Support rapid implementation of new legislative requirements for benefits including TRICARE Reserve Select refinement, traumatic Service Member’s group life insurance, care for wounded warriors, expanded care for autistic children
- Support process improvement, transformation, and adaptive planning by implementing system changes and contract transitions in support of the next round of contracts between TRICARE Management Activity (TMA) and the Managed Care Support Contractors (MCSC)
- Accurately tracks contingency personnel statistics based on location
- Provide expanded identity and person/patient search services, and reengineering and improvements to line of duty injury processes and systems for injured reservists as well as rapid implementation of innovations in prevention and wellness, and wounded warrior support
- Provide military and retiree personnel and pay data to the Department of Veterans Affairs (VA)
- Transfer dependent survivor pay and family SGLI data to VA for the purpose of providing benefits for VA Loans, Pension or Dependency Indemnity Compensation (DIC), Dependent Educational Assistance Program (DEA), and insurance payment/burial benefits upon death of a family member.
- Accurately tracks policy coverage data for non-TRICARE health insurance policies that cover eligible DEERS beneficiaries, for instance, through their civilian employers

The foundation for Future Improvements in Personal Identity Verification (PIV) and Sharing Data with Veterans Affairs (VA) – a key e-Gov initiative

- Automated resolution of conflicting identity information about medical beneficiaries
- Health care contractor disposition of health care notifications and other mailings sent to military health care beneficiaries

The backbone of customer outreach programs reinforcing the Department’s goal of a lifetime relationship with the entire DoD family to maximize prevention, wellness and personal choices and responsibility. Supports over 9 million beneficiaries including the 3 million individuals stationed in more than 140 countries, and their families, that are dedicated to deterring and defeating the enemy. For example:

- DMDC Support Office assists DoD beneficiaries who have questions about their DEERS records and DoD benefits, answering over 60,000 calls per month. Annually they coordinate and send over 6 million letters or notifications to military sponsors, their family members and beneficiaries covering impact on their medical benefits upon celebrating significant birthdays, enrollment and disenrollment into TRICARE health care plans, and evidence of their prior healthcare coverage under one of the TRICARE-administered programs
- Coordinates with the TRICARE Management Activity to educate the TRICARE-eligible population—including military retirees and their beneficiaries—on congressionally mandated changes in medical entitlements, such as purchase options for Medicare prescription drug coverage
- Annually sends mobile verification teams to locations such as the Philippines to support veterans, family members and survivors who reside in that country
- Customer Care Teams assists beneficiaries who have exceptional concerns or issues that affect their DEERS record or benefits, escalating problematic situations that often require collaboration with other Federal Agencies for resolution

Support the Warfighting Commands. DMDC provides critical decision support for the combatant commands and joint force commanders to securely share information across multiple domains, ranging from intelligence to personnel systems. The result is integrated information for quick and decisive action.

- Contingency Tracking System (CTS) - tracks the deployment of over 1.5 million Service members who served in over 2 million deployment events supporting Operations

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

Enduring Freedom/Iraqi Freedom. CTS provides current information for war planners and helps ensure Service members receive benefits authorized.

- Critically wounded patients from the warfronts are flown to Landstuhl Regional Army Medical Center in Germany to stabilize before they return to the U.S. Some of these heroes are unable to leave the hospital to replace their CACs lost in battle. DMDC Support Group-Europe makes regular visits to Landstuhl and uses deployable equipment to produce CACs without requiring wounded troops to leave their hospital rooms.
- DNA Registry, Personnel locator, Panograph retrieval (full mouth dental x-rays) of military members, and Fingerprint registry and retrieval
- Language capabilities and qualifications locator and registry
- Real-time mobilization support for Guard/Reserve and their families
- Personnel TEMPO and sustaining the force initiatives
- Force structure analysis
- Retention/attrition/accession quality and numbers
- Certification of job skills and experience acquired on active duty that may apply to post service employment
- Processing of military funeral honors requests via phone, and the web
- DoD workforce planning and military casualties information
- Statistics on contract actions, top 100 DoD contractors, procurement details by geographic locations, commodity groups and reporting component, historical procurement trends, subcontracting data and DoD grants
- Defense Biometric Identification System (DBIDS) – a force protection capability deployed worldwide

RAPIDS is the network of over 2,600 issuing stations at 1,700 locations that provides the uniformed Services the means to verify one's eligibility for specific benefits and entitlements. Verifying officials at RAPIDS sites are DoD's agents who positively identify those eligible for benefits/entitlements, then generate DoD credentials for those in uniform, DoD civilians, DoD contractors and other eligible DoD credential holders. RAPIDS is the designated system in the DoD for entry of family members into DEERS ensuring eligible family members are appropriately categorized and issued identification credentials that correctly reflect their entitlements and privileges. RAPIDS positions fixed, mobile and forward deployed sites in such locations as Iraq, Afghanistan, Kuwait, Qatar, Djibouti, the Balkans, and on Navy ships. RAPIDS also integrated a new Central Issuance Facility (CIF). The CIF capability is deployed at all Service basic training facilities and Academies. RAPIDS collects the required information and forwards it to a high-speed printer at the CIF. CACs are securely returned within 48 – 72 hours. .

Common Access Card (CAC). The CAC is DoD's enterprise-wide solution for secure identity credentials allowing physical and logical access. CAC uses the DEERS-based Person Data Repository database for authentication and personnel information. Once the identities of uniformed Service members, DoD civilians, and selected contractors are verified, they are issued CACs containing digital certificates for logical access to DoD's computer networks and systems, and physical access to buildings and controlled spaces. 2.4 million CACs are issued annually. On average, CAC's are issued in 15 minutes, including the time to encode digital certificates onto the CAC. Annually 175,000 CACs are produced at the Central Issuance Facility. As a direct result of the use of Public Key Infrastructure (PKI) certificate on the CAC to log onto DoD networks, the number of successful attacks on the DoD network was reduced by 46%.

Retiree and Family Member ID Cards. Two thirds of all DoD ID cards support our Military retirees and DoD Military family members. ID cards are issued at RAPIDS and take less than 7 minutes to produce. As results are seen from the use of PKI on the CAC for Military members, future enhancements to the retiree and family member ID cards

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

will be made as economics and business case dictates. There are 6.2 million retirees and family member ID cards in circulation.

CAC is the cornerstone for Project ePurse. Recruits in training will no longer have to carry cash. DMDC, working jointly with the Department of Treasury, successfully deployed an ePurse pilot project with the Marine Corps, involving 529 recruits at Parris Island, SC and Camp Pendleton, CA. A stored value "purse" is initialized on their CAC from funds in recruit's payroll account and is used to purchase items at the Base Exchange. Expenditures are debited instantly from the recruit's payroll account. Remaining funds are returned to the recruit's account after four months. Future use of the ePurse include Navy shipboard activities that require hard currency, the Army Eagle Cash, as well as other existing cash card programs that may benefit by using the CAC as their cash card.

The flagship for identity management and authentication services promoting the Presidential initiatives for e-Government and Homeland Security. The Personnel Identity Protection (PIP) program places the Department in a leadership position on identity management. The PIP is the DoD's proactive approach, using DEERS and the DEERS infrastructure, to protect the identities of our Service members, employees, and families while securing access to Government assets through strong identity authentication.

DMDC is using digital technology to link to DEERS and validate the credentials of users who are authorized access to a computer application, a government building, or a military installation. To further the goal of protecting the identity of our military members and their families, DoD civilian employees, affiliates, and contractor partners, the Department leveraged DEERS by developing and enhancing additional identity protection systems to implement the PIP. These systems include Defense Biometric Identification System (DBIDS), Defense National Visitors Center (DNVC), and Defense Cross-Credentialing Identification System (DCCIS).

Force Protection for safer military bases. As the CAC has been instrumental in reducing the number of successful attacks on the DoD network, employment of a modular, secure, rules-based access control system supported by rapid electronic authentication has enhanced the overall security posture of the Department's bases, stations and facilities. The Defense Biometric Identification System (DBIDS) is a Personnel Identity Protection initiative that uses existing DoD-issued identification credentials to authorize approved cardholders physical access on a scalable level. Because of the interoperable, regional nature of DBIDS, access decisions can be based on real-time authentication of the cardholder's status. In those cases where card termination and revocation decisions made at one activity have historically not been available to other locations, a terminated credential can be flagged and access denied when presented at another location. Given the Department's involvement in the Global War on Terror, and the need to assure the protection of our deployed forces, CENTCOM has recognized DBIDS as the access control solution that will be installed at sites and installations across Southwest Asia. DBIDS is deployed across EUCOM, is installed at many of the forward locations in PACOM, and has just been recognized as the access control solution in defense of the homeland by NORTHCOM. DBIDS provides an effective, real time solution to the thousands of lost, stolen and counterfeit identity credentials that are presented at DoD gates and access control points around the world in an effort to gain unauthorized access for reasons ranging from simple fraud, to potential acts of terror. Statistically:

- DBIDS recorded 250 million accesses to military installations between January 2005 and December 2007, denying access in 1.5 million cases with numerous incidents where DBIDS was responsible or instrumental in identifying individuals engaged in criminal activity.
- Over 1.5 million people are registered in DBIDS and 280,000 DBIDS cards have been issued. DBIDS uses existing DoD-issued identification credentials to authorize only approved cardholders' physical access on a scalable level including access to a given building, installation or an entire theater of operations
- DBIDS is used at 300 gates at 162 installations in Korea, Europe, Japan, South West Asia, and the Continental United States.

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

Enabling Visitor Centers and Cross-Credentialing. DNVC is the Government to Business authentication solution. DNVC allows use of the DoD credential, an employee ID and fingerprint, as well as an approved federated credential to validate in real time against an approved DoD authoritative data source. At an access control point the DNVC operator receives a picture of the credential holder and a fingerprint match score. Based on evaluation of this information, the visitor is authorized access to the facility. DCCIS authenticates commercial industry credential holders at DoD facilities and DoD ID credentials at commercial facilities providing real-time authentication and notification of terminated credentials among its federated partners.

Implementing Homeland Security Presidential Directive 12 (HSPD-12). Under HSPD-12 (Policy for a Common Identification Standard for Federal Employees), the President directed a common, interoperable identity credential across the federal government's Executive Branch. Thanks to DMDC's technical guidance and assistance, DoD has led the federal enterprise's response to this directive. The existing Common Access Card provides a single, interoperable credential across DoD. Transition to the next generation technology meets the required technical criteria, allowing DMDC to continue to raise the bar on physical and logical access control, to enhance DoD's overall security posture, and concurrently reach a level of interoperability with other federal departments and agencies. The new DoD CAC is supported by rapid electronic authentication of the cardholder's identity. The capability to provide this real-time authentication enables credential cross-recognition, thereby reducing the requirement for duplicate/redundant badging systems, the costs of sustaining independent identity management systems, and improving the credential's trustworthiness. The real benefit to the federal government is the increased assurance of secure logical and physical access control.

- Supporting Homeland Security in natural disasters, such as hurricanes Katrina and Rita. Noncombatant Evacuation Operations (NEO) Tracking System (NTS) is an automated hardware and software package that helps warfighters and joint task force commanders conducting noncombatant evacuation operations by giving them visibility over evacuees as they move through the evacuation pipeline. The Automated Repatriation Reporting System (ARRS) is a web-based tool supporting the Department of the Army as the Executive Agent for Repatriation. ARRS can be used to track and support evacuees following repatriation after NEO.
- ARRS tracks OCONUS-based military personnel and their family members who made emergency trips in 2005 to the Southeast U.S. in the wake of hurricanes Katrina, Rita, and Wilma
- NTS uses hand-held scanners and other devices to collect personal information on evacuees at registration stations from identification documents, such as CACs, passports and other military IDs. Data is quickly and accurately transmitted from the enrollment station to the central NTS database at DMDC, using satellite communications. Evacuees are issued bar-coded wristbands for scanning at intermediate stops. Evacuees are tracked through the evacuation pipeline, through temporary or intermediate safe havens, back to the U.S.
- Over 500 portable NTS kits are employed worldwide by PACOM, EUCOM, other combatant commands, United States Forces Korea and Japan, PACAF, the 25th Infantry Division (Light) in Hawaii, and III Marine Expeditionary Force (Okinawa)
- DMDC is also implementing a Personnel Accountability and Reporting system (PARS) to allow the Services and Defense Agencies to retrieve a 'baseline population' of DoD affiliated individuals potentially affected by disasters, such as the 2007 wildfires in southern California and to capture and report to Joint Staff their subsequent status.

Implementing an E-Authentication Program. In 2005, the General Services Administration asked DoD to participate in the federal E-Authentication program to expand the electronic government initiative in the President's Management Agenda. DMDC leveraged a logical access solution to support DoD family members and retirees. The CAC issued to uniformed service members and civilian employees contains an identity credential imbedded into an integrated chip. This credential provides a secure means to authenticate to online services. Other members of DoD, such as retirees and family members, do not carry such a credential. In order to access their benefits online, they must establish new accounts and passwords at every site they visit, forcing them to maintain dozens of different accounts and passwords. A single identity account and password,

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

called the Family Account, was required to enable family members and others without a CAC to access their online benefits. The Family Account is now a fully accredited E-Authentication credential service provider. It is one of only two such accredited systems in DoD and among just a handful in the entire federal government. It will be used by the Military Healthcare System to provide access to online benefits. Moreover, uniformed Service members and their families can now safely and securely access their benefits online from home, without maintaining dozens of different accounts.

Ensuring federal tax dollars are expended lawfully. Based on data matches with the Defense Finance and Accounting Service, the Department of Veterans Affairs, the U.S. Department of Health and Human Services (HHS), and individual states, DMDC identified potential fraud or erroneous payments by current and prior DoD-affiliated members and contract vendors. For example:

- As a result of a data match performed by the Defense Manpower Data Center (DMDC) DFAS is collecting \$336,000 from military retired pay accounts reported for members who also had received involuntary separation pay benefits. There are an additional \$3M in retired pay accounts for which preliminary research indicates that the members also received separation pay. DFAS has recommended that the retirement pay center implement the DMDC matching program to identify these duplicate payments.
- As a result of a review of involuntary separation pay benefits for members who later received VA disability-related compensation, DMDC and DFAS validated 1,790 cases valued at \$31.2M where members receive both benefits. The VA Compensation and Pension Service performed their initial review and found 22% of the referrals will require offset of VA Compensation by the amount of the Military Separation Pay. If the VA is successful in offsetting these amounts the projected benefit is \$6.8M.
- Based on inputs from 44 state public assistance agencies and coordination with HHS, DMDC conducted computer matches under the auspices of the Public Assistance Reporting Information System (PARIS) that identified 580,590 duplicate records, indicating potential fraud in one quarter's match. The voluntary PARIS program verifies client-reported entitlement eligibility for individual federal block grants.
- Data was provided to VA for the 54,006 reservists who also receive VA benefits so that pay for 4.6 million drill days and active duty days can be offset from their VA benefits.

Helping to select the highest quality recruits and match people to the best job. DMDC's staff of measurement professionals conducts all phases of testing, from test development to test delivery for measures designed for diverse populations (including high school students, military applicants, enlisted military personnel, and military linguists).

- DMDC develops the Armed Services Vocational Aptitude Battery (ASVAB), a test designed to select and classify military applicants. DMDC successfully introduced a Computer Adaptive Testing (CAT) versions in 1990. To date, over 3 million people have taken the CAT-ASVAB. The average CAT-ASVAB test time is about two hours, versus about four hours for the old paper and pencil ASVAB.
- In the Global War on Terror, DoD needs more people proficient in foreign languages. DMDC has taken the DoD lead in developing an automated delivery system for Web-based Defense Language Proficiency Tests, or DLPT, including reading and listening proficiency tests in multiple foreign languages. To date, over 20,000 people have taken the Web-based DLPT; once fully deployed, about 50,000 people will be tested annually. DMDC maintains the centralized DLPT database and conducts centralized scoring and program management. The DLPT test delivery technology improves test score accuracy, provides better test security, and increases both the proficiency and understanding of DoD's language skills. This enhances DoD's intelligence collection capabilities and effectiveness on the battlefield.
- DMDC provides career exploration materials—including an interest inventory and ASVAB test forms—to over 700,000 high school students in 13,000 schools annually, helping them learn more about career exploration and planning. This career exploration program provides the Services with recruiting leads for high scoring students and gives high school students state-of-the-art career exploration materials.

**Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008**

DCPDS:

FY 2007

- Deployed Spiral 1.2 to approximately 51,000 personnel, bringing NSPS total to over 100,000
- Completed HR/payroll feasibility study.
- Initiated action to consolidate hardware operations.
- Continued to improve Self Service capabilities.

FY 2008

- Initiate plan for consolidation of DCPDS server operations.
- Initiate action to meet the GIG milestone objectives.
- Complete CAC-enablement and a Reduced Sign-on (RSO) capability for DCPDS Self Service
- Initiate a CNDSP Service Level Agreement with Army Research Lab to support DCPDS operations

FY 2009

- Upgrade to Itanium processors enterprise- wide
- Initiate consolidation of DCPDS regional server operations
- Initiate an integrated HR/Payroll prototype

Major Planned Activities

DEERS/RAPIDS/CAC:

DEERS/RAPIDS/CAC Performance Goals:

- Continue the highest standards of accuracy for over 35 million records and worldwide access times for over 3 million transactions processed daily
- 99.5% availability for the database outside of scheduled maintenance
- Posting of updated information from the Uniformed Services no more than 24 hours from receipt
- Support of Service member mobilizations within 24 hours of notification
- Reduce average issuance times to no more than 15 minutes for all DoD Identification card forms;
- 97% availability for the RAPIDS system, as measured as an aggregate, across all locations
- Incorporate new benefits or entitlements as directed by Congressionally mandated dates
- Ensure card technology remains state-of-the-art, interoperable, and sufficiently secure to facilitate e-Government and secure electronic transactions
- Meet Presidential mandates in accordance with DoD approved plan for HSPD-12
- Facilitate smart card program implementation by other Government agencies and pioneer smart card technology advancement within the Federal Government via support for the Government Smart Card FIPS-201 standards sponsored by the National Institute of Standards and Technology (NIST)

**Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008**

- Maintain User Outreach Program to promote usage of the CAC and PK-enabled application development, provide information and presentations to the user community, and plan major educational events at least 4 times per year
- Provide essential post-issuance capability
- Provide beneficiaries and their family members with a central support office for assistance with updating their DEERS record to ensure they receive entitlements and benefits
- Enhance customer care by collaborating with Federal Agencies such as the Social Security Administration, and the Centers for Medicare and Medicaid Services, to ensure member benefits are protected
- Answer beneficiary phone calls in under one minute wait time
- Answer beneficiary correspondence within ten days
- Create a team to proactively identify and fix data errors, before beneficiaries are negatively impacted
- Create and retain accurate reporting required by law or regulation for educational programs, verification of military experience and training, actuarial data, PERSTEMPO, linguist tracking, child and spouse abuse, federal parent locator, and Defense incident reporting which feeds the National Incident Based Reporting System, EEO, Census, and demographics data
- Support backend authentication protocols to promote interagency interoperability
- Participate in Coalition partner pilots using the CAC
- Issue new DoD populations ID cards so they can authenticate on DoD networks securely and physically access DoD installations to receive their entitlements
- Work with the medical community to use the CAC as an authentication token for scheduling medical appointments and receiving their drug benefits at the pharmacies.
- Complete recurring DoD reports and publications on schedule and within congressionally mandated deadlines
- Identify possible fraud in the Department via Fraud Focus - an on-going tri-agency effort to minimize fraud and abuse against DoD financial assets. Summary statistics (both cumulative since inception and cumulative for the current fiscal year) of quantifiable benefits attributable to Fraud Focus, covering Civilian Pay, Military Pay, Retired/Annuitant Pay, Vendor Pay, Data Mining, Contract Pay, Cross System, Purchase Card, and Transportation are:

	Cumulative (since 8/5/1994)	FY 2007 (thru June 2007)
Erroneous Payment	\$134,681,280	\$ 695,288
Suspected Fraud	\$ 6,821,423	\$1,373,244
Actual Fraud	\$ 10,053,556	\$ 0
Cost Avoidance	\$ 10,398,455	\$ 459,687
Total	\$161,954,714	\$ 2,528,219

- Minimize fraud via computer matches with SSA resulting in prosecutions and cost recovery totaling \$2.6 million
- Work with the Army and Air Force Exchange Service (AAFES) and Navy Exchange (NEX) Service allowing the catalog exchange service to receive real-time, automated verification of eligibility determination for Web catalog sales

DCPDS:

- Activities planned for FY 2008 and FY 2009 include the planning for and initiation of the Consolidation of DCPDS hardware and operations. CPMS will capitalize and

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

consolidate the databases distributed and operated by the Components into a consolidated platform owned by CPMS, locating them at the DCPDS operation at the Lockheed Martin Denver Data Center. The architecture at this single location would be a consolidated center containing all of the Component regional HR databases. The systems integrator would provide a fully integrated environment for Consolidated DCPDS that would include network communications, database administration, system administration, systems engineering, information assurance and disaster recovery. An initial HR/Payroll integration prototype is planned for FY 2009.

- With the completion of the Human Resources/Payroll Business Case Analysis, the efficiencies for an integrated system have been clearly demonstrated. The modernization of the payroll system and integration with DCPDS would eliminate multiple databases and manual workarounds, improve response time, and result in significant savings with a benefit to cost ratio of 3.45 to 1.
- CPMS will continue upgrading DCPDS data warehouse to support enhanced user access to and timeliness of civilian HR information. Further enhancements in DCPDS Self-Service for all DoD employees are already underway, making HR information accessible to DoD employees, managers and supervisors.
- DCPDS will migrate the enterprise-wide system to the Itanium processor in FY 2009, a significant upgrade affecting all DCPDS server operations.

Global Information Grid (GIG) / Net-Centricity

DEERS/RAPIDS/CAC:

DEERS is in compliance with the DoD Net Centric Data Strategy of December 2001. DEERS has expanded to focus on the visibility and accessibility of data and to respond to increasing performance standards. DEERS is migrating to a Java 2, Enterprise Edition, (J2EE) platform, Service Oriented N-Tier Architecture, including presentation, business, data integration and resource tiers, to service all of DMDC's operational needs. This initiative includes:

- Architectural design for re-use via model-driven architecture
- Shared infrastructure
- Standardized deployment strategy
- Uniform application monitoring for Service Level Agreement (SLA)
- Dissemination of information across projects
- Guidelines for good design and development practices
- Use of enterprise architectural design patterns
- Migration of existing web services to unified offering for discovery of service offerings
- Distributed computing as an enterprise architectural strategy
- Business process discovery

DEERS has completed an updated Enterprise Architecture (EA) Transition Strategy in FY08 to be integrated into the DoD-wide EA Transition Plan in the Human Resources Mission Area. As part of the transition to Net Centric capability, DEERS is preparing for registration of Structural, Services and Content Metadata in DoD enterprise repositories, as they become available.

Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008

DCPDS:

DCPDS is the largest fully deployed automated HR enterprise system providing HR information and system support for the DoD civilian workforce worldwide replacing multiple legacy systems and supporting over 800,000 employee records. It supports appropriated and non-appropriated fund employees; local national and National Guard Bureau personnel via 22 DoD Regional Service Centers and over 300 Customer Support Units worldwide. DCPDS was designed to improve and simplify personnel transaction processing the delivery of personnel services and retrieval of timely civilian workforce information. CPMS is responsible for functional and technical oversight of DCPDS to include system upgrades and enhancements. Deployment of the system began in October 1999 reaching FOC on September 27, 2002.

**Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008**

Information Technology Budget Exhibit Resource Summary by Initiative (IT-1)

	----- Dollars in Thousands -----			
	<u>FY2007</u>	<u>FY2008</u>	<u>FY2009</u>	<u>FY2010</u>
DEFENSE HUMAN RESOURCES ACTIVITY RESOURCE SUMMARY:	141,311	133,050	206,854	216,622

0573 - DEFENSE CIVILIAN PERSONNEL DATA SYSTEM (DCPDS)

Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - CIVILIAN PERSONNEL

Operations

			----- Dollars in Thousands -----			
<u>Appropriation</u>	<u>Budget Activity</u>	<u>Budget Line Item</u>	<u>FY2007</u>	<u>FY2008</u>	<u>FY2009</u>	<u>FY2010</u>
O&M,DEF-WIDE	BA 04 ADMN & SRVWD ACT	DOD HUMAN RESOURCES ACTIVITY	37,826	19,804	44,717	76,613

Procurement

			----- Dollars in Thousands -----			
<u>Appropriation</u>	<u>Budget Activity</u>	<u>Budget Line Item</u>	<u>FY2007</u>	<u>FY2008</u>	<u>FY2009</u>	<u>FY2010</u>
PROC., DEF-WIDE	BA 01 MAJOR EQUIPMENT	PERSONNEL ADMINISTRATION	4,003	2,886	13,392	4,196

RDT&E

			----- Dollars in Thousands -----			
<u>Appropriation</u>	<u>Budget Activity</u>	<u>Program Element</u>	<u>FY2007</u>	<u>FY2008</u>	<u>FY2009</u>	<u>FY2010</u>
RDT&E,DEF-WIDE	BA 06 RDT&E MGMT SUPPORT	0901220SE PERSONNEL ADMINISTRATION	0	0	15,700	0

Initiative Resource Summary:	41,829	22,690	73,809	80,809
-------------------------------------	---------------	---------------	---------------	---------------

4035 - DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM (DEERS)

Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - HEALTH

Operations

			----- Dollars in Thousands -----			
<u>Appropriation</u>	<u>Budget Activity</u>	<u>Budget Line Item</u>	<u>FY2007</u>	<u>FY2008</u>	<u>FY2009</u>	<u>FY2010</u>
O&M,DEF-WIDE	BA 04 ADMN & SRVWD ACT	DOD HUMAN RESOURCES ACTIVITY	96,002	106,880	129,104	131,821

**Department of Defense
Fiscal Year (FY) 2009 IT President's Budget Request
February 2008**

Information Technology Budget Exhibit Resource Summary by Initiative (IT-1)

4035 - DEFENSE ENROLLMENT ELIGIBILITY REPORTING SYSTEM (DEERS) (Continued)

Major

GIG Category: FUNCTIONAL AREA APPLICATIONS - HEALTH

Procurement

			----- Dollars in Thousands -----			
<u>Appropriation</u>	<u>Budget Activity</u>	<u>Budget Line Item</u>	<u>FY2007</u>	<u>FY2008</u>	<u>FY2009</u>	<u>FY2010</u>
PROC., DEF-WIDE	BA 01 MAJOR EQUIPMENT	PERSONNEL ADMINISTRATION	3,480	3,480	3,941	3,992
Initiative Resource Summary:			99,482	110,360	133,045	135,813