Report No. D-2009-005 October 10, 2008

Inspector General
United States Department of Defense

Controls Over the Contractor Common Access Card Life Cycle

Additional Information and Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms and Abbreviations

AMC	Army Materiel Command
CAC	Common Access Card
CVS	Contractor Verification System
DEERS	Defense Enrollment Eligibility and Reporting System
DMDC	Defense Manpower Data Center
DUSA-BT	Deputy Under Secretary of the Army for Business Transformation
GS	General Schedule
ILP	Inventory Logistics Portal
JPAS	Joint Personnel Adjudication System
KBR	Kellogg, Brown, and Root, Inc.
NACI	National Agency Check with Inquiries
RAPIDS	Real-Time Automated Personnel Identification System
SES	Senior Executive Service
SPOC	Service Point of Contact
TASM	Trusted Agent Security Manager
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD (P&R)	Under Secretary of Defense for Personnel and Readiness

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

October 10, 2008

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Controls Over the Contractor Common Access Card Life Cycle
(Report No. D-2009-005)

We are providing this report for review and comment. We considered comments from clients on a draft of this report when we prepared the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. We reviewed comments from the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Personnel and Readiness; the Under Secretary of Defense for Intelligence; the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer; the Commander, U.S. Army Materiel Command; the Deputy Under Secretary of the Army for Business Transformation; the Director, Defense Manpower Data Center; and the Adjutant General, U.S. Army Human Resources Command.

After receiving client comments, we met with representatives from the Offices of the Secretary of Defense, the Under Secretary of Defense for Personnel and Readiness, and the Deputy Under Secretary of the Army for Business Transformation. As a result of these meetings, we added two recommendations and revised four recommendations. Our clients agreed to take additional actions not addressed in their responses to the draft report. On the basis of these agreements, we consider the recommendations generally resolved; however, they remain open for reporting purposes pending receipt and review of comments on the final report. We added Recommendation A.1. and renumbered draft Recommendations A.1. through A.5. as A.2. through A.6. We renumbered draft Recommendation B.3. as B.4. after adding a new B.3. We revised Recommendations A.3.a.(2), A.3.b.(2), B.2., and C.1.c. We request additional comments on the added and revised recommendations, as well as on Recommendations A.3.a.(1)(b), A.3.b.(1), A.3.c., B.1.a., B.1.b., C.1.a., C.1.b., C.2.a., and C.2.b., by October 31, 2008. Please see the recommendations table on page ii for responsible organizations.

Please provide comments that conform to the requirements of DoD Directive 7650.3. If possible, send your comments in electronic format (Adobe Acrobat file only) to AudJ&OO@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to Ms. Melinda M. Oleksa at (703) 604-9174 (DSN 664-9174) or Ms. Hanh T. Nguyen at (303) 676-7397 (DSN 926-7397). Team members are listed inside the back cover.

Paul J. Granetto
Principal Assistant Inspector General
for Auditing

DISTRIBUTION:

DEPUTY SECRETARY OF DEFENSE
UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
ASSISTANT SECRETARY OF DEFENSE (NETWORKS AND INFORMATION INTEGRATION)/DOD CHIEF INFORMATION OFFICER
COMMANDER, U.S. ARMY MATERIEL COMMAND
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
NAVAL INSPECTOR GENERAL
DEPUTY UNDER SECRETARY OF THE ARMY FOR BUSINESS TRANSFORMATION
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
DIRECTOR, DEFENSE MANPOWER DATA CENTER
ADJUTANT GENERAL, U.S. ARMY HUMAN RESOURCES COMMAND

Results in Brief: Controls Over the Contractor Common Access Card Life Cycle

The life cycle of the contractor Common Access Card (CAC) consists of approval, issuance, reverification, revocation, and recovery. DoD officials use the Contractor Verification System (CVS) to approve contractor CACs, and the Real-time Automated Personnel Identification System (RAPIDS) to issue CACs.

What We Did

The objective of this audit was to determine whether controls over contractor CACs were in place and worked as intended. This audit is the first in a series on contractor CACs.

What We Found

Additional controls over contractor CACs are needed, and existing controls need improvement. Specifically, contractor CACs were not consistently approved, issued, reverified, revoked, or recovered across DoD.

- Government sponsors had inadequate evidence to link contractors to a contract or justify a CAC expiration date.
- Some contractors received CACs without undergoing background checks or receiving appropriate Government approval.
- CAC issuers changed information approved by Government sponsors.
- DoD did not always recover revoked contractor CACs.

Also, better Army oversight is required for a Kellogg, Brown, and Root, Inc. (KBR) RAPIDS site that issued 25,428 CACs to contractors deploying to Southwest Asia.

- A KBR subcontractor did background checks with no Army oversight.
- A contractor facilitated a CAC approval process that bypassed CVS.
- Nearly half of revoked CACs were not recovered.

Contractors were misclassified as Government employees on their CACs. Specifically, 40,055 contractor CACs indicated the holders had General Schedule pay grades, and 211,851 had e-mail addresses that improperly identified the holders as U.S. Government employees.

Also, contractors could become CVS sponsors, and sponsors who left Government service may have been approving CACs.

Overall, CAC life-cycle weaknesses pose a potential national security risk that may result in unauthorized access to DoD resources, installations, and sensitive information worldwide.

What We Recommend

To tighten controls over contractor CACs, we recommend implementing:

- joint, DoD-wide, contractor CAC life-cycle policy;
- improved Army oversight at the KBR CAC issuance site;
- additional system controls for CVS and RAPIDS; and
- procedures to ensure CAC sponsors are current Government employees.

Client Comments and Our Response

Clients generally concurred with the recommendations. One outstanding item remained, which related to implementing systems controls to reject improper e-mail addresses for contractors applying for a CAC. As a result of management and client comments, we added, revised, and renumbered recommendations. For the recommendations requiring additional comments, please see the table on the back of this page.

Recommendations Table

Client	Recommendations Requiring Comment	No Additional Comments Required
Deputy Secretary of Defense	A.1.	
Under Secretary of Defense for Acquisition, Technology, and Logistics		A.2., A.5., and D.2.
Under Secretary of Defense for Personnel and Readiness	A.3.a.(1)(b), A.3.a.(2), A.3.b.(1), A.3.b.(2), A.3.c., C.1.a., C.1.b., C.1.c., C.2.a., and C.2.b.	A.3.a.(1)(a), A.3.d., A.3.e., A.5., and D.2.
Under Secretary of Defense for Intelligence	C.2.a. and C.2.b.	A.4., A.5., D.2.
Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer	C.2.a. and C.2.b.	
Commander, U.S. Army Materiel Command	B.1.a., B.1.b., and B.2.	B.1.c. and B.1.d.
Deputy Under Secretary of the Army for Business Transformation	B.3.	
Director, Defense Manpower Data Center		A.6. and D.1.
Adjutant General, U.S. Army Human Resources Command		B.4.

Please provide comments by October 31, 2008.

Table of Contents

Table of Contents (cont'd)

Client Comments

Introduction

Objectives

The overall objective of this audit was to determine whether controls over Common Access Cards (CACs) provided to contractors were in place and worked as intended. Specifically, we determined whether DoD officials issued CACs to contractors, verified the continued need for contractors to possess CACs, and revoked and recovered CACs from contractors in accordance with DoD policies and procedures.

Background

In October 2000, DoD began issuing CACs to active-duty military personnel, reserve personnel, civilian employees, and eligible contractors. DoD personnel and eligible contractors use CACs as a general identification card and to gain access to DoD resources, installations, and sensitive information. In addition, CACs allow DoD personnel and eligible contractors to electronically sign and send encrypted e-mails to facilitate daily business activity. Under the Geneva Conventions, the CAC also serves as an identification card for civilians and contractors who accompany the Armed Forces during a conflict, combat, or contingency operation. Figure 1 summarizes CAC responsibilities of DoD agencies according to DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," July 19, 2004, and the Web site of the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD [AT&L]).

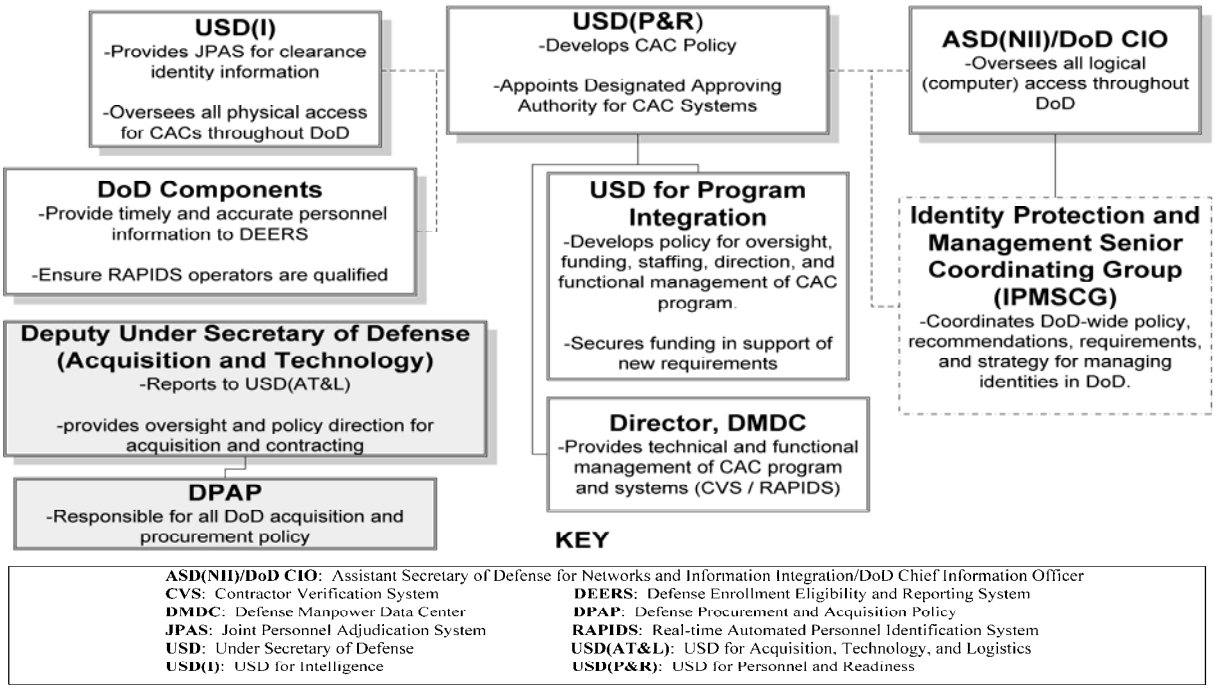


Figure 1. CAC Responsibilities of DoD Agencies

As shown in Figure 1, the responsibilities for implementing and overseeing the CAC program are spread among many DoD agencies, requiring extensive coordination. DoD has not established a lead agency to control overall CAC implementation.

Contractor CACs

A contractor CAC looks different from military and DoD civilian CACs. It displays a green vertical[1] stripe and contractor affiliation, allowing Government officials to differentiate a contractor's access privileges to DoD resources, installations, and information from civilian or military access privileges. See Figure 2 for CAC samples.

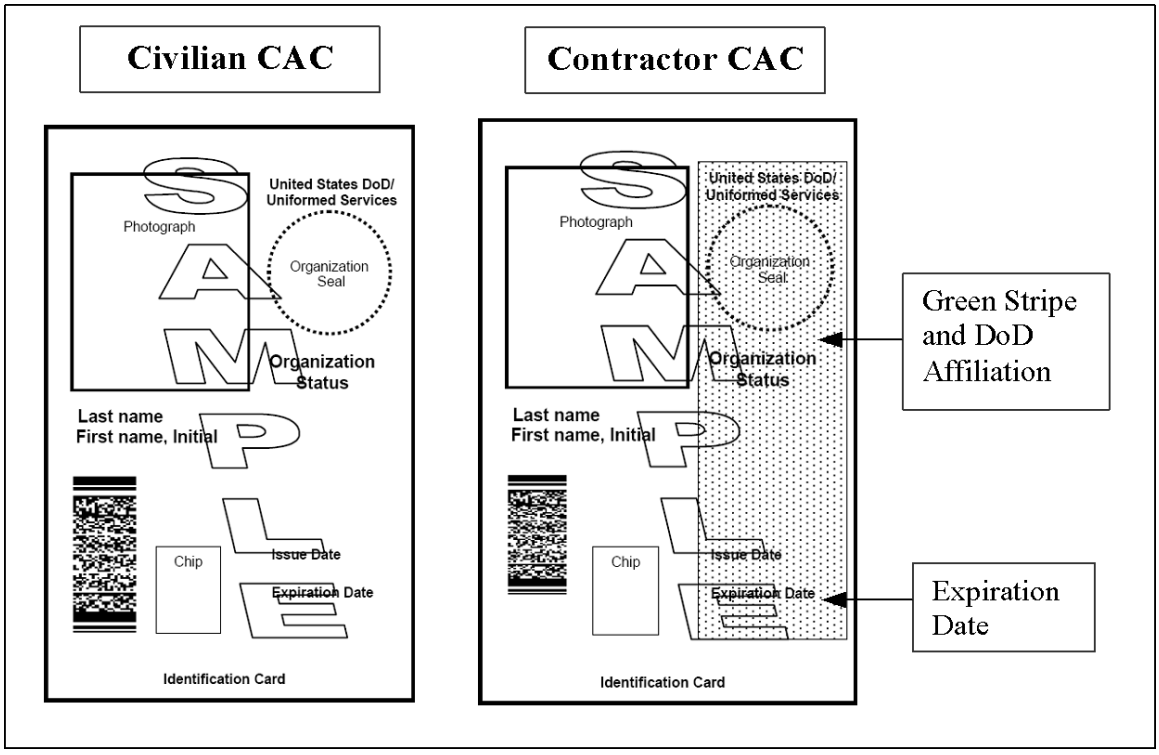


Figure 2. Samples of Civilian and Contractor CACs

An Office of the Secretary of Defense Memorandum signed by the Under Secretary of Defense for Personnel and Readiness (USD [P&R]) and the DoD Chief Information Officer, "Common Access Card (CAC)," January 16, 2001, implemented CAC policy for a common identification card intended to grant access to DoD facilities and networks. This policy was updated in an Office of the Secretary of Defense Memorandum signed by USD (P&R) and the DoD Chief Information Officer, "Common Access Card—Changes," April 18, 2002.

[1]DMDC stated that the new Homeland Security Presidential Directive-12 CAC has a green horizontal stripe to indicate a contractor.

Systems Used To Process Contractor CACs

A memorandum from USD (P&R), "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005, mandates the use of the Contractor Verification System (CVS) to approve contractors' applications for CACs. CVS is a Web-based system that feeds information on approved contractors into the Defense Enrollment Eligibility and Reporting System (DEERS), the central repository for information collected about DoD personnel and their authorized beneficiaries.

A second system, the Real-time Automated Personnel Identification System (RAPIDS), retrieves contractor records from DEERS and prints the information on CACs for issuance.

Reliance on Computer-Processed Data

We relied on computer-processed data for the numbers and percentages in the findings. In finding A, we used statistical sampling estimates, which we identified by using the word "estimate" before stating the percentage. Some numbers and percentages in finding A were not based on statistical estimates, and therefore we did not use the word "estimate" to describe these. Findings B, C, and D did not use statistical estimates. Appendix A explains how computer-processed data were used and our assessment of their reliability.

Subsequent Common Access Card Audits

This audit is the first in a series on the contractor CAC. The second in the series focuses on the contractor CAC in Southwest Asia. The third in the series focuses on the contractor CAC in the Republic of Korea. Subsequent CAC audits may be planned for other overseas locations.

The Federal Acquisition Regulation 2.101 states that an "Inherently Governmental Function means, as a matter of policy, a function that is so intimately related to the public interest as to mandate performance by Government employees." Some of the identified weaknesses in this report may be related to contractors performing inherently governmental functions. This issue will be included in subsequent audits.

Finding A. Policy Governing the Contractor Common Access Card Life Cycle

Contractor CACs were not consistently approved, issued, reverified, revoked, or recovered across DoD. These CAC life-cycle weaknesses pose a potential national security risk that may result in unauthorized access to DoD resources, installations, and sensitive information worldwide. To improve national security, DoD should implement policy governing CACs from approval to recovery. The policy should require:

- Government sponsors to coordinate with contracting and security personnel before approving contractor CACs,
- system controls for CVS and RAPIDS to prevent improper changes to contractor CAC records, and
- a clause in DoD contracts to encourage CAC recovery.

Phases of the CAC Life Cycle

The contractor CAC life cycle consists of four phases: application approval, issuance, reverification, and revocation and recovery. The application approval phase begins when a contractor requests a CAC through CVS. After the CVS application is approved, the contractor reports to a RAPIDS site for CAC issuance. After issuance, CAC reverification occurs in CVS every 180 days to ensure the contractor continues to need a CAC. Finally, the CAC revocation and recovery phase begins when contractors no longer need or are authorized CACs. Figure 3 displays the phases, and Figure 5 shows a detailed chart of the contractor CAC life cycle.

CVS Approval Phase	RAPIDS Issuance Phase	CVS Reverification Phase	CVS/RAPIDS Revocation and Recovery Phase
• Government sponsors confirm contractors' need for CACs and approve applications using CVS • CVS electronically updates contractors' records in DEERS	• RAPIDS personnel verify contractors' identity and check DEERS to ensure contractors have an approved CVS application • RAPIDS personnel issue CACs	• Every 6 months, CVS requires contractors' CAC need to be reverified • If the need is not reverified, contractors' CACs are revoked	• When contractors no longer need their CACs, they should be revoked in either CVS or RAPIDS • The CACs should also be recovered

Figure 3. Phases of the Contractor CAC Life Cycle

Management of CAC Life Cycle Phases

As noted in the introduction, the responsibilities for implementing and overseeing the CAC program are spread among many DoD agencies. Those responsibilities also vary by phase in the contractor CAC life cycle. DoD has not established a single agency to control overall CAC implementation—including physical and logical access, background checks, and systems controls—to ensure that contractors seeking CACs to gain access to DoD resources and information are properly vetted, authorized, and monitored.

Statistical Samples

Each phase of the CAC life cycle has unique functions; therefore, we used statistical sampling to audit each phase. The Defense Manpower Data Center (DMDC) provided four contractor CAC data populations that corresponded to each phase of the contractor CAC life cycle. We grouped the data geographically to determine the locations with the most contractor CAC activity for each DoD Component.[2] We used these locations as our subpopulations for statistical sampling. We relied on the Office of Inspector General Quantitative Methods Directorate to randomly select a sample for each subpopulation. See Appendix A for additional information about the statistical samples.

For each statistical sample, we tested specific steps in the CAC life cycle. On the basis of the test results, the Office of Inspector General Quantitative Methods Directorate estimated the number of deficiencies in each subpopulation. These estimates include an interval with upper and lower bounds using a 90-percent confidence level. We are 90-percent confident that the number of deficiencies in the CAC life cycle lies within an estimated range of the subpopulation; there is a 10-percent risk that the true value is outside the interval. Finding A reports the point estimate of each sample (middle of upper and lower bounds); see Appendix B for additional information on the estimates based on each statistical sample. Table 1 summarizes the details of each sample.

Table 1. Statistical Sampling of Contractor CACs by Phase

Data Populations Provided by DMDC	Total Records	Records in Subpopulation	Subpopulation as a Percent of Total	Sample Size
CVS applications	126,331	39,532	31%	235
CACs issued	462,952	97,117	21%	145
CVS reverifications	61,492	32,098	52%	160
CACs revoked	175,037	28,205	16%	250

Approval of Contractors' Applications for CACs

According to the USD (P&R) Memorandum, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005 (hereafter referred to as the P&R Memorandum), as of

[2]DoD Components include the Army, the Navy, the Air Force, the Marine Corps, and DoD agencies.

July 2006 contractors who need CACs are required to apply for them electronically using CVS. Each contractor should be sponsored by a Government official, also known as a Trusted Agent,[3] who is authorized to enter information into CVS.

Before approving contractors' applications for CACs in CVS, Trusted Agents must do the following.

- Establish the contractor's affiliation with the Government through contract requirements in accordance with the Federal Information Processing Standards Publication 201-1, "Personal Identify Verification (PIV) of Federal Employees and Contractors," March 2006, and DMDC CVS User Training Guide, Version 1.9, July 19, 2007.[4]

- Establish the contractor's need for logical and physical access and the duration of access to DoD networks or facilities in accordance with the DMDC CVS User Training Guide, Version 1.9, July 19, 2007.

- Verify that the contract companies have vetted their contractors' backgrounds[5] in accordance with the DMDC CVS User Training Guide, Version 1.9, July 19, 2007.

Contractor Affiliation With DoD

An estimated 82.93 percent of 39,532 CVS applications did not adequately document contractors' affiliations to the referenced DoD contracts (see Appendix B for the detailed estimate). The P&R Memorandum did not indicate how Trusted Agents should validate a contractor's affiliation and did not require Trusted Agents to retain information supporting CAC applications.

Based on interviews with Trusted Agents at 32 CVS sites, a contractor's DoD affiliation was established through several means, such as:

- visit authorization letters[6] from contract companies that requested contractor CACs for access to DoD resources, installations, and information to perform contract services, and

---

[3]Trusted Agents were often Government contracting personnel or security managers. In many instances, they held other Government positions, such as financial managers and administrative staff.

[4]Version 1.7, issued in September 2006, contained the same guidelines.

[5]Background checks are discussed under the issuance phase because the approval of an application does not necessarily result in a CAC being issued.

[6]Visit authorization letters contained contractor information such as name, Social Security number, date of birth, contract number, and security clearance level.

- requests by telephone or e-mail from contractor employees or Government contracting personnel for a CAC.

However, supporting documentation and explanations provided by Trusted Agents did not confirm that contractors with CACs had legitimate DoD affiliations. Examples follow.

- At one CVS site, a Trusted Agent stated that, under the Privacy Act, he was not permitted to maintain any personal information; therefore, he did not provide any supporting documentation related to the referenced contracts proving that contractors he sponsored had a valid DoD affiliation.

- At another CVS site, a Trusted Agent stated that she destroyed CAC application forms because there was no requirement to retain them.

- At other CVS sites, several Trusted Agents stated that they had personal knowledge of which contractors needed CACs, even though some of the Trusted Agents were responsible for hundreds of contractors.

Also, 2,560 of the 126,331 CVS applications provided by DMDC from January 1 through June 30, 2007, did not reference a valid contract number. For example, "n/a" is not a valid contract number.

CAC Expiration Dates

An estimated 89.50 percent of 39,532 CVS applications did not have sufficient evidence to support that CAC expiration dates were within the scope of DoD contract periods of performance (see Appendix B for the detailed estimate). The Office of the Secretary of Defense Memorandum signed by USD (P&R) and the DoD Chief Information Officer, "Common Access Card (CAC)—Changes," April 18, 2002 (hereafter the CAC Memorandum), allows CACs to be issued for a period of 3 years or the individual's term of service, employment, or association with DoD, whichever is shorter. However, Trusted Agents could not provide supporting documentation that showed their contractors were associated with DoD contracts for a specific period of performance. Instead, Trusted Agents used various methods to establish the contractor CAC expiration date. For example, a Trusted Agent stated that he used the end date of the last option year of a contract as the CAC expiration date. Another Trusted Agent stated that she approved CACs for 2 years past the contract end date.

To reduce CAC issuance workload, the Army and Navy DEERS/RAPIDS program offices instructed their RAPIDS personnel, by e-mail, to issue contractor CACs for a period of 3 years regardless of the contractors' terms of service. Until CVS reverification and recovery are proven to function correctly across DoD, CAC expiration dates should be established in accordance with DoD guidance.

Issuance of CACs

According to RAPIDS Site Security Managers[7] at 35 locations, contractors report to a RAPIDS station, specifically to RAPIDS Verifying Officials[8] at the same locations, to obtain their CACs. After verifying the contractor's identity, the Verifying Official uses the contractor's Social Security number to retrieve the contractor's record from DEERS. If the contractor's DEERS record indicates that the contractor is sponsored through CVS, the Verifying Official issues the CAC. If the contractor does not have a DEERS record or the record does not indicate that the contractor is sponsored through CVS, the Verifying Official directs the contractor to the CVS Trusted Agent to appropriately resolve the matter.

Background Checks

According to data obtained from the Joint Personnel Adjudication System (JPAS), Trusted Agents approved an estimated 40.49 percent of 97,117 contractor CACs without verifying that background checks had been initiated or completed for the contractors (see Appendix B for the detailed estimate). The P&R Memorandum does not require Trusted Agents to confirm with a Government security office that contractor background checks have been initiated or completed before approving their CVS applications. Trusted Agents stated that they did not confirm that background checks for contractors had been initiated or completed because:

- contract companies were responsible for obtaining proper background checks for their employees,
- contractors did not work on classified contracts, and
- Government security officers were responsible for background checks.

Although a security clearance is not required to obtain a CAC, Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004, and Federal Information Processing Standard 201-1 require contractors seeking a CAC to have a National Agency Check with Inquiries (NACI) or an equivalent background investigation. Officials from the Office of the Under Secretary of Defense for Intelligence stated that a National Agency Check with Local Records and Credit Check, or a NACLC, is an equivalent investigation. DoD Regulation 5200.08-R, "Physical Security Program," April 9, 2007, also requires a NACI or an equivalent investigation for permanent issuance of the CAC. Accordingly, we relied on the Office of Inspector General Personnel Security Office to check JPAS and

---

[7]A RAPIDS site cannot operate without a Site Security Manager, who is responsible for user and site administration, management of CAC stock, policy and procedure compliance, documentation and training, and future CAC issuance enhancements.

[8]Verifying Officials operate RAPIDS stations and issue CACs to contractors. Verifying Officials can be Government officials or contractors.

verify whether contractors who were issued a CAC had a NACI or an equivalent background check.[9] We did not search other systems because DoD Directive 1000.25, "DoD Personal Identity Protection (PIP) Program," July 19, 2004, designates JPAS as the DoD personnel security clearance system. JPAS maintains all types of personnel clearance actions, including initial requests for background checks.

Government Approval

RAPIDS personnel issued an estimated 16.19 percent of 97,117 contractor CACs without the required Government approval (see Appendix B for the detailed estimate). RAPIDS did not have the controls to prevent CAC issuance to contractors who were not sponsored in CVS.

The P&R Memorandum states that, as of July 31, 2006, CAC issuance to contractors should be accomplished using CVS. However, Verifying Officials issued numerous CACs before this effective date using DD Form 1172-2, "Application for Department of Defense Common Access Card DEERS Enrollment." Specifically, contractors requesting access to DoD facilities and networks completed a DD Form 1172-2 and submitted it to a Government sponsor. When the Government sponsor approved and returned the form to contractors, they then reported to a RAPIDS station. The RAPIDS Verifying Official issued the contractors their CACs based on the DD Form 1172-2 information. If a contractor did not have a personnel record in DEERS, the Verifying Official created a DEERS record for the contractor. If the contractor already had a DEERS record, the Verifying Official ensured the information was up-to-date and issued the CAC. If the DD Form 1172-2 was not complete or approved, the Verifying Official required the contractor to obtain an appropriate form from the sponsor. Verifying Officials later forwarded the DD Forms 1172-2 to the DMDC Support Office for storage.

As of October 2007, one of the Army RAPIDS sites was still accepting the DD Form 1172-2 for CACs instead of applications submitted electronically through CVS. See finding B for details of the continued use of DD Form 1172-2.

The DMDC Support Office could not provide a CAC application that showed evidence of Government approval either through CVS or DD Form 1172-2 for 18 of 145 contractor CACs. Of the 18 contractor CACs, 4 were issued in 2007, after the CVS mandate took effect.

CAC Reissuance

According to the CAC Memorandum, CAC reissuance occurs when CACs are lost, stolen, or damaged or when information printed on the CAC requires change. Several RAPIDS Site Security Managers stated that they reissue CACs to contractors who report the cards missing as long as contractors have a valid DEERS record.

---

[9]See Appendix A for additional information about our reliance on the Office of Inspector General Personnel Security Office, and finding B for additional information on background investigation requirements.

Based on the DMDC data spanning January 1 through June 30, 2007, 4,309 of the 151,984 revoked CACs were coded as "lost."[10] It was not clear whether these contractors who lost CACs were eligible for reissuance. Therefore, when reissuing a CAC, the Verifying Officials should confirm that Trusted Agents have reestablished a contractor's continued affiliation with DoD in CVS.

Issuance of Multiple Active Contractor CACs

As of July 19, 2007, DMDC data showed 772 U.S. and foreign national contractors with multiple active CACs, totaling 1,545 CACs. Appendix C details the number of contractors and CAC types. In the CAC Memorandum, DoD acknowledges that there are individuals who have multiple affiliations with the Department, such as a reservist who is also a DoD contractor. However, DoD has not developed a solution for issuing a single CAC regardless of the number of affiliations.

Although a contractor may have both a contractor and a military reservist CAC, it does not seem logical that a contractor should possess two contractor CACs. The DMDC data showed a contractor who had two active contractor CACs—one Identification CAC and one Identification and Privilege CAC.[11] The complexity of CAC affiliations and the number of contractors with multiple CACs may prevent DoD from accurately accounting for its contractors overseas or in the United States.

Consistency of Contractor CAC Information

The RAPIDS Verifying Officials issued an estimated 29.45 percent of 97,117 contractor CACs with information different from that approved by the Government sponsor through CVS/DD Form 1172-2 (see Appendix B for the detailed estimate). Specifically, contractor CAC information such as pay grades, e-mail addresses, and expiration dates[12] differed between DEERS/RAPIDS and CVS/DD Form 1172-2 (see Table 2 for details). Reasons for differences were that CVS did not include all fields from DD Form 1172-2, such as pay grade and Geneva Conventions category, and that RAPIDS did not have automated system controls to prevent Verifying Officials from changing contractor information entered or approved by the Trusted Agent in CVS.

---

[10]We ascertained this by querying the DMDC database on the revoke code, a character in DEERS that explains why a CAC was revoked. For example, revoke code "L" means the CAC was lost.

[11]A DoD Identification and Privilege CAC entitles the holder to exchange and commissary privileges, access to recreation facilities, and military discounts.

[12]See finding A, page 8, for a discussion of expiration dates.

Table 2. Inconsistencies in the Sample of 145 CACs Issued to Contractors

Name	Pay Grade	Geneva Conventions Category	E-mail Address	Duty Country	CAC Expiration Date
2	2	3	30	9	9

In one case, a Trusted Agent approved a contractor CAC for expiration on June 30, 2007; however, a RAPIDS Verifying Official changed the expiration date to May 29, 2010. Another CAC application had no expiration date, and the Verifying Official issued a 3-year CAC. In both cases, the Verifying Officials had no authority to set or extend the contractor's CAC expiration date. As previously discussed, contractors' CAC applications should be approved by Trusted Agents in CVS. When Verifying Officials believe that there is an error in a contractor's CAC application, they should direct the contractor to see his or her Trusted Agent so that appropriate changes are made.

Reverification of CACs

CVS was implemented to facilitate better tracking of contractor CACs than was possible with the manually processed DD Form 1172-2. One improvement to the process in CVS was the programmed prompt to reverify contractor CACs. Specifically, the DMDC CVS User Training Guide states that the Trusted Agent should reverify a contractor's need for a CAC every 180 days. When a contractor reaches the 150-day mark, the Trusted Agent receives e-mail notification from CVS to reverify the contractor's continued need for the CAC. The Trusted Agent has 30 days after this notification to reverify, or the contractor's CAC will automatically be revoked.

An estimated 92.04 percent of 32,098 CVS reverifications did not have sufficient evidence to support the contractors' continued need for CACs (see Appendix B for the detailed estimate). The P&R Memorandum did not require Trusted Agents to confirm with contracting officials the contractors' continued need for CACs or to maintain evidence of such confirmation. Therefore, Trusted Agents performed reverification in many different ways. For example, Trusted Agents stated that they:

- checked JPAS, Army Knowledge Online, the Microsoft global e-mail address list, and local installation or facility badging systems to determine whether contractors continued working with the Government, and

- recognized contractors' faces and assumed that contractors still needed CACs.

Some Trusted Agents sponsored many contractors while carrying out other duties. Trusted Agents' workload may have contributed to the lack of strong reverification procedures.

Approximately 91.2 percent of 6,282, or 5,727 Trusted Agents, sponsored 50 or fewer contractors from January 1 through June 30, 2007. However, the remaining 8.8 percent,

or 555 Trusted Agents, sponsored an average of 117 contractors during this period; Table 3 has details.

Table 3. Sponsorship Load of Trusted Agents During the First 6 Months of 2007

Number of Contractors Sponsored per Trusted Agent	Number of Trusted Agents With This Load
1 – 10	4,017
11 – 25	1,117
26 – 50	593
51 – 100	364
101 – 250	155
251 – 500	27
501 – 1,000	7
More than 1,200	2

Because there are no standard procedures for reverification, it is difficult to estimate how long a reverification would take. Therefore, a reasonable limit on the number of contractors a Trusted Agent may sponsor could not be established. However, DoD should strengthen the reverification control by examining additional ways to establish a reasonable number of contractors a Trusted Agent may sponsor.

In addition, the CVS User Training Guide did not specify procedures for the Trusted Agents to reverify their contractors' CACs. Rather, the Guide states:

> To reverify a contractor's authorization to hold a CAC, click on the "Reverify" button. When the "Reverify" button is clicked, a pop-up window will appear . . . which asks you to confirm that you would like to reverify the applicant's privileges to continue to carry a CAC. Click "OK" to process the verification request.

Figure 4 illustrates the reverification pop-up window.

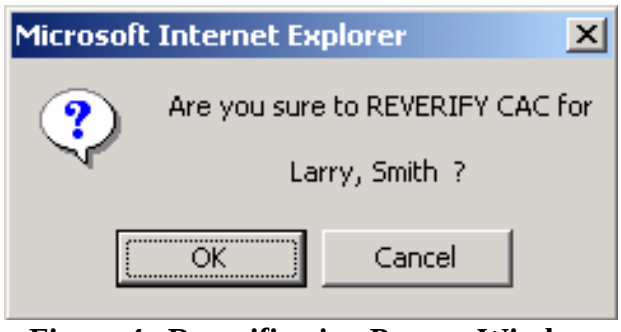


Figure 4. Reverification Pop-up Window

Because Trusted Agents may have had too many contractors and CVS reverification required only clicking a button, sponsors may not have spent much time or effort on

reverification. Further, because documentation is lacking, DoD has no assurance that the Trusted Agents performed the reverification thoroughly and consistently across DoD.

Revocation and Recovery of Contractor CACs

The CAC Memorandum states that invalid, inaccurate, inoperative, or expired CACs shall be returned to a RAPIDS site for disposition. When they receive the CACs, the RAPIDS Site Security Managers submit the CACs to DMDC. When DMDC receives them, DMDC updates their status in the Inventory Logistics Portal (ILP), the system for inventory and logistic management of CAC cardstock. This action indicates that the CACs have been revoked, recovered, and prepared for destruction.

Recovery Procedures

DoD officials did not recover an estimated 37.85 percent of 28,205 revoked CACs. In addition, we could not determine whether DoD recovered an estimated 19.91 percent of the 28,205 revoked CACs (see Appendix B for the detailed estimate). The CAC and P&R Memoranda do not outline specific procedures for collecting revoked CACs. In addition, the CAC and P&R Memoranda do not specify procedures for following up with companies whose contractors do not return their CACs. Many Trusted Agents expressed concerns about their responsibilities for recovering CACs. Examples follow.

- Because contractors worked at different locations, Trusted Agents were unaware of contractors leaving until after the fact. Thus, recovering CACs was difficult.

- Trusted Agents revoked contractors' records in CVS, but felt it was not their job to collect CACs.

Further, the CAC and P&R Memoranda do not assign responsibility for recovering contractor CACs. Trusted Agents stated that:

- contractors were required to turn in their CACs to the companies, and

- Government contracting personnel were responsible for retrieving the CACs.

Contract Clause

DoD did not have a contract clause to make contractor companies aware that CACs need to be returned upon employees' termination, resignation, or completion of service. Of the nine[13] Federal and DoD acquisition regulations reviewed, two[14] contained clauses that

[13](1) Federal Acquisition Regulation, (2) Defense Federal Acquisition Regulation Supplement, (3) Army Federal Acquisition Regulation Supplement, (4) Navy-Marine Corps Acquisition Regulation Supplement, (5) Air Force Federal Acquisition Regulation Supplement, (6) Air Force Materiel Command Federal Acquisition Regulation Supplement, (7) Air Force Space Command Federal Acquisition Regulation Supplement, (8) Defense Logistics Acquisition Directive Federal Acquisition Regulation Supplement, and (9) U.S. Special Operations Command Federal Acquisition Regulation Supplement.

could be inserted in DoD contracts for governing the CAC recovery process (see Appendix D for details of the regulations). However, those regulations were vague, leaving contracting officials to determine whether the clauses should be included in the contracts.

U.S. Law Governing Identification Cards

Unauthorized possession of an official identification card, like a CAC, can be prosecuted criminally under section 701, title 18, United States Code. It states:

> Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both.

CAC recovery may improve if, during the CVS application process, applicants were informed of this law and told that once they no longer had a valid need for CACs or that their CACs were revoked or expired, they must return CACs to responsible Government officials.

Directive-Type Memoranda

DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007, states that Directive-Type Memoranda shall be effective for no more than 180 days from the date signed, during which time they shall be incorporated into an existing DoD issuance, converted to a new DoD issuance, reissued, or canceled.[15] Our research of DoD issuances showed neither the P&R Memorandum nor the CAC Memorandum has been incorporated in or converted to a DoD issuance, reissued, or canceled. Because both of these memoranda were issued more than 180 days ago and have not been cancelled, they should be incorporated in or converted to a DoD issuance.

Conclusion

DoD did not have policies and procedures that consistently governed the contractor CAC life cycle. Specific weaknesses follow.

- Trusted Agents did not establish contractors' DoD affiliations and CAC expiration dates before approving CVS applications.

---

[14]Federal Acquisition Regulation 52.204-9, "Personal Identity Verification of Contractor Personnel," November 2006, and Air Force Federal Acquisition Regulation Supplement, Clause 5352.242-9001, "Common Access Cards (CACs) for Contractor Personnel," August 2004.

[15]A DoD issuance is a DoD Directive, Instruction, or Regulation.

- Trusted Agents approved CVS applications without verifying a background check.

- Verifying Officials issued contractor CACs without Government approval and with information that differed from what the Trusted Agents had approved in CVS.

- Trusted Agents did not consistently reestablish contractors' continued need for CACs before reverifying the CACs in CVS.

- DoD officials did not recover all contractor CACs that were revoked.

These CAC life-cycle weaknesses pose a potential national security risk that may result in unauthorized access to DoD resources, installations, and sensitive information worldwide. See Figure 5 at the end of this finding for a summary of the contractor CAC life cycle.

Actions Taken by the Defense Manpower Data Center

DMDC officials stated that they started exploring solutions for CAC recovery in July 2008. Specifically, they are studying ways to make contractors aware of CAC recovery requirements through both CVS and RAPIDS. Also, DMDC officials stated that they would continue to look for ways to encourage contractors and contracting organizations to return CACs when they are revoked.

Recommendations, Client Comments, and Our Response

Added, Renumbered, and Revised Recommendations

As a result of management and client comments, we added Recommendation A.1. to establish a lead office responsible for the CAC life cycle, and renumbered draft Recommendations A.1. through A.5. as A.2. through A.6. In addition, we revised draft Recommendations A.2.a.(2) and A.2.b.(2)—now A.3.a.(2) and A.3.b.(2)—to clarify the intent of the recommendations. Specifically, Recommendation A.3.a.(2) was revised to clarify the need to ensure that certain data fields from the DD Form 1172-2 are included as data fields in CVS, and are subsequently completed and transferred to DEERS/RAPIDS by the Trusted Agents. Also, Recommendation A.3.b.(2) was revised to clarify the need for Verifying Officials to ensure that the contractor, when attempting to replace a lost CAC, is still eligible and has a continued need for a CAC by coordinating with the responsible Trusted Agent.

A.1. We recommend that the Deputy Secretary of Defense designate an office with the authority and responsibility for overseeing the DoD contractor Common Access Card life cycle, including implementation of policy for logical and physical access.

A.2. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics direct the Defense Acquisition Regulations Council to include a standard contract clause in the Defense Federal Acquisition Regulation Supplement that, at a minimum, requires contractors to comply with the joint Common Access Card policy in Recommendation A.5. This clause should be applicable to all DoD contracts and subcontracts for which contractor or subcontractor personnel receive Common Access Cards.

Client Comments

The Principal Deputy Director, Acquisition Resources and Analysis, responding for the USD (AT&L), agreed. The Principal Deputy Director stated that USD (AT&L) plans to open a Defense Federal Acquisition Regulation Supplement case to add appropriate regulatory language making contractors accountable for any CACs issued to them, including returning the CACs if the CAC holder no longer needs or is no longer authorized to use the CAC.

Our Response

The Principal Deputy Director's comments were responsive, and no additional comments are required.

A.3. We recommend that the Under Secretary of Defense for Personnel and Readiness:

a. Implement system controls for the Contractor Verification System and the Real-time Automated Personnel Identification System to prevent improper changes to contractor Common Access Card records. System controls should, at a minimum:

(1) Prevent the Real-time Automated Personnel Identification System from:

(a) Issuing Common Access Cards to contractors without the approval of a Trusted Agent in the Contractor Verification System.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed. The Deputy Under Secretary stated that, in October 2008, DMDC will enforce the lock down of DEERS/RAPIDS data entry so that data on contractors applying for CACs are entered through CVS.

Our Response

The Deputy Under Secretary's comments were responsive, and no additional comments are required.

(b) Modifying contractor Common Access Card information approved by the Trusted Agent. When Verifying Officials believe there is an error in a contractor's record, they should direct the contractor to see his or her Trusted Agent so changes may be made.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), partially agreed. The Deputy Under Secretary stated that, as indicated in the response to Recommendation A.3.a.(1)(a), DMDC will lock DEERS/RAPIDS data entry and see that, as of October 2008, contractor data are entered only through CVS. The Deputy Under Secretary stated that the lock down would prevent DEERS/RAPIDS Verifying Officials from modifying contractor eligibility data (specifically, the CAC expiration date) without approval from the Trusted Agent in CVS. Further, the Deputy Under Secretary stated that, to accurately manage identity in DEERS, certain data fields would remain open for update by the Verifying Official in accordance with DEERS/RAPIDS procedures (for example, name change due to marriage where a scanned marriage certificate is required in DEERS).

Our Response

The Deputy Under Secretary's comments were partially responsive. We agree that the lock down is intended to prevent Verifying Officials from modifying contractor data without approval from the Trusted Agent in CVS, and we acknowledge the need for certain data fields to remain open for modification by the Verifying Official (such as a name change due to marriage). However, the Deputy Under Secretary did not specify which data fields would remain open or the rationale for keeping those fields open for modification by the Verifying Official. We request that the USD (P&R) provide comments on the final report by October 31, 2008, specifying the RAPIDS data fields that will remain open and the rationale for allowing Verifying Officials to modify those data fields.

(2) Ensure that data fields from the DD Form 1172-2, such as the pay grade and Geneva Conventions category, are added to the Contractor Verification System, and that Trusted Agents subsequently and accurately complete and transfer all fields to the Defense Enrollment Eligibility and Reporting System/Real-time Automated Personnel Identification System.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed, stating that the October 2008 DEERS/RAPIDS lock down should help ensure that data entered into CVS are accurately transferred to DEERS/RAPIDS.

Our Response

The Deputy Under Secretary agreed; however, we concluded from the response that our recommendation was unclear. As a result, we revised the recommendation to clarify the

need to ensure that certain data fields from the DD Form 1172-2 are included as data fields in CVS, and are subsequently completed and transferred to DEERS/RAPIDS by the Trusted Agents. We request that the USD (P&R) review the revised recommendation and provide comments on the final report by October 31, 2008.

b. Implement procedures to prevent:

(1) Contractors from having multiple active contractor Common Access Cards, unless one is for military service.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed in principle, stating that such procedures have already been implemented by DoD. The Deputy Under Secretary stated that it is possible for an individual to be a DoD civilian, Military Service reservist, adjunct professor, and contractor at the same time, with each personnel category qualifying an individual for a separate CAC. However, the Deputy Under Secretary stated that it is DoD policy to issue only one active CAC per personnel category, including contractors, and all RAPIDS versions currently enforce this policy.

Our Response

Although the Deputy Under Secretary agreed, we consider the comments nonresponsive. We acknowledge that, according to DoD policy, only one active CAC can be issued per personnel category. However, as of July 19, 2007, our analysis of DMDC data showed that 772 U.S. and foreign national contractors had multiple active contractor CACs (see Appendix C for details of the number of contractors and CAC types). Because our analysis of the data shows that this DoD policy is not consistently implemented throughout the Department, we request that the USD (P&R) provide comments on the final report by October 31, 2008, addressing specific actions that will be taken to ensure that the DoD policy for issuing one active CAC per contractor is implemented and enforced.

(2) Verifying Officials from reissuing contractor Common Access Cards when contractors report them as "lost" unless the Verifying Officials coordinate with responsible Trusted Agents to confirm whether the contractors still have a valid need for Common Access Cards.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), disagreed. The Deputy Under Secretary stated that the current process requires CVS Trusted Agents to reverify contractors' continued affiliation with DoD and need for a CAC every 6 months, making any additional reverification redundant. The Deputy Under Secretary further explained that the USD (P&R) will establish and publish guidelines with steps the Trusted Agent must take to reverify a record in conjunction with the policy that is under development.

Our Response

The Deputy Under Secretary's comments were nonresponsive; however, we concluded from the response that our recommendation was unclear. As a result, we revised the recommendation to clarify the need for Verifying Officials to ensure that the contractor, when attempting to replace a lost CAC, is still eligible and has a continued need for a CAC by coordinating with the responsible Trusted Agent. We request that the USD (P&R) review the revised recommendation and provide comments on the final report by October 31, 2008.

c. Implement a process that periodically informs Trusted Agents (Government sponsors) when their contractors have not turned in revoked Common Access Cards.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), disagreed. The Deputy Under Secretary stated that her office recognizes that there are challenges associated with the retrieval of revoked CACs, but that implementing an automated means to periodically inform Trusted Agents when CACs have not been returned will not help with tracking revoked cards. Instead, the Deputy Under Secretary stated that DoD established mechanisms to account for virtually 100 percent of the CACs that are revoked—to include cards reported lost or stolen, not functioning properly, terminated due to separation, or expired—and that these cards are shown as inactive within the CAC issuance system and certificates are revoked by the DoD Public Key Infrastructure. The Deputy Under Secretary further stated that, although DoD can account for a majority of the cards that have been returned to DMDC for disposition, some cards cannot be physically accounted for because they were lost or stolen, no longer functional, or worn beyond recognition. The Deputy Under Secretary explained that periodic reports to CVS Trusted Agents on CACs reported as not returned could potentially include revoked cards that were returned and properly destroyed. As a result, the Deputy Under Secretary recognized the need to improve procedures for the return of CACs as a controlled item, including tighter contractual obligations, but stated that this would be done using policy and oversight efforts associated with revocation and retrieval of CACs instead of automated methods.

Our Response

The Deputy Under Secretary's proposed corrective actions are partially responsive. Specifically, we acknowledge the Deputy Under Secretary's recognition of the need for improved procedures for the return of CACs as a controlled item, including tighter contractual obligations, and that policy and oversight efforts, if properly enforced, will facilitate the retrieval of revoked CACs. However, for the Deputy Under Secretary's comments to be fully responsive, we request that the USD (P&R) provide comments on the final report by October 31, 2008, specifying the policy and oversight efforts that will be implemented to enforce the revocation and retrieval of CACs.

d. Require the Army and Navy Defense Enrollment Eligibility and Reporting System/ Real-time Automated Personnel Identification System program

offices to rescind the guidance for issuing 3-year Common Access Cards regardless of the contractors' terms of service. Rather, the Army and Navy Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System program offices should direct issuance of Common Access Cards in accordance with DoD policy.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed, stating that the Defense Human Resources Activity Identification Card Policy Office sent e-mails to the DEERS/RAPIDS Service project offices to ensure that contractor CACs are issued with expiration dates in accordance with current policy. The Deputy Under Secretary also stated that she believed the DEERS/RAPIDS Service project offices rescinded any guidance that was contrary in nature.

Our Response

The Deputy Under Secretary's comments were responsive, and no additional comments are required.

e. In accordance with DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007:

(1) Incorporate or convert Under Secretary of Defense Memorandum, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005, into a DoD issuance, reissue the memorandum, or cancel it.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed, stating that as the designated lead for the implementation of Homeland Security Presidential Directive-12, the USD (P&R) will incorporate the USD (P&R) Memorandum, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005, as well as any additional CAC-related policies under the USD (P&R), into new issuances currently in development. The Deputy Under Secretary also stated that the new issuances include the draft Deputy Secretary of Defense Directive-Type Memorandum 08-006 and the draft USD (P&R) Directive-Type Memorandum 08-003 that outline the Department's roles and responsibilities for CAC and Homeland Security Presidential Directive-12-related items within the scope of the audit. Finally, the Deputy Under Secretary stated that, as required by DoD Directive 5025.01, "DoD Directives Program," October 28, 2007, these Directive-Type Memoranda will be converted into a DoD instruction within 180 days of their release and will include any unaddressed policy-related items associated with controls over contractor CACs to the maximum extent possible.

Our Response

The Deputy Under Secretary's comments were responsive, and no additional comments are required.

(2) Coordinate with the DoD Chief Information officer to incorporate or convert Office of the Secretary of Defense Memorandum, "Common Access Card (CAC)," January 16, 2001, into a DoD issuance, reissue the memorandum, or cancel it.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed and addressed the planned corrective actions in the response to Recommendation A.3.e.(1).

Our Response

The Deputy Under Secretary's comments were responsive, and no additional comments are required.

A.4. We recommend that the Under Secretary of Defense for Intelligence implement policy that, at a minimum, specifies background investigation requirements and the method and system needed to verify the results of the background investigations for both U.S. and foreign national contractors who will be issued Common Access Cards.

Client Comments

The Under Secretary of Defense for Intelligence neither agreed nor disagreed. However, the Under Secretary stated that Federal standards mandate the NACI as the minimum background investigation for Homeland Security Presidential Directive-12 credentialing. The Under Secretary stated that interim credentials may be issued upon a favorable fingerprint check and the submission of the requisite investigation, that they are reviewing solutions to facilitate electronic verification of background investigations, and that they expect implementation by the end of 2009. The Under Secretary also stated that, in partnership with the Office of the Secretary of Defense, the Services, and agency staff, his office is working on policy guidance that will outline the investigative requirement for CAC credentialing throughout DoD. The Under Secretary added that CAC credentialing standards will apply to all DoD employees, Military Services, contractors (in staff-like positions requiring logical access), and other DoD personnel requiring physical access for 6 months or more. Finally, the Under Secretary stated that specific guidance to establish credentialing and background investigation standards for foreign nationals (non-U.S. citizens, including contractors) is under development with the Department of State, and that CAC issuance to foreign nationals will be limited and strictly controlled.

Our Response

The Under Secretary's comments were responsive, and no additional comments are required.

A.5. We recommend that the Under Secretary of Defense for Personnel and Readiness, Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Under Secretary of Defense for Intelligence:

a. Designate within 90 days the lead organization responsible for developing and implementing a joint contractor Common Access Card policy (also see Recommendation D.2.).

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed, stating that the USD (P&R) is the lead for Homeland Security Presidential Directive-12, which includes coordination of the policies associated with CAC issuance, and that policy development is underway to address the items outlined in the recommendation.

The Principal Deputy Director, Acquisition Resources and Analysis, responding for the USD (AT&L), agreed, stating that the USD (AT&L) will work with the USD (P&R) and the Under Secretary of Defense for Intelligence to implement these recommendations.

The Under Secretary of Defense for Intelligence partially agreed, stating that as the Principal Staff Assistant for Physical Security (access control), Personnel Security (background investigations), and the National Industrial Security Program (contractors), his office would, in coordination with the USD (P&R) and the USD (AT&L), develop policy for the DoD CAC for their areas of responsibility. In addition, the Under Secretary stated that contractors who are not eligible for the DoD CAC will receive a local or a DoD alternate, physical-access-only credential, which is under development. Additionally, the Under Secretary stated that his office is developing separate, comprehensive security policy for all categories of individuals requiring access to DoD-owned and -controlled facilities worldwide, which will mandate minimum access control standards, procedures, and equipment, including requirements for contractors.

Our Response

The Deputy Under Secretary's, Principal Deputy Director's, and Under Secretary's comments were responsive, and no additional comments are required.

b. Implement the joint policy, which at a minimum should require:

(1) Trusted Agents to coordinate with contracting and security personnel when establishing contractors' initial and continued affiliation with DoD and need for Common Access Cards, and to maintain evidence of this coordination.
(2) Standard procedures resulting from Recommendation A.4. for confirming background checks for contractors applying for Common Access Cards.
(3) A limit on the number of contractors a Trusted Agent may sponsor.

(4) Trusted Agents to follow up with contractors who have not returned their Common Access Cards once Recommendation A.3.c. is implemented.
(5) Specific Government personnel to recover contractor Common Access Cards when they are no longer needed.
(6) Trusted Agents to inform security personnel when contractors do not return revoked Common Access Cards. In addition, security personnel should consider taking action under section 701, title 18, United States Code.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed with Recommendations A.5.b.(1), (2), (3), (5), and (6), stating that policy development is underway to address these items. The Deputy Under Secretary disagreed with Recommendation A.5.b.(4), stating that although she recognizes the challenges associated with CAC retrieval, instead of attempting to implement the automated notifications referenced in A.3.c., the USD (P&R) will coordinate and establish CAC retrieval policies and procedures.

The Principal Deputy Director, Acquisition Resources and Analysis, responding for the USD (AT&L), agreed, stating that the USD (AT&L) will work with the USD (P&R) and the Under Secretary of Defense for Intelligence to implement these recommendations.

The Under Secretary of Defense for Intelligence agreed, stating that his office will implement appropriate policy as referenced and will address physical security requirements for CACs as controlled, U.S. Government property that requires the protection of personally identifiable information; a reporting requirement for lost or stolen credentials; and referral to the Department of Justice for violations of section 701, title 18, United States Code and section 797, title 50, United States Code.

Our Response

Although the Deputy Under Secretary disagreed with Recommendation A.5.b.(4)., the proposed corrective action to coordinate and establish CAC retrieval policies and procedures satisfied the intent of this recommendation. Therefore, the Deputy Under Secretary's, Principal Deputy Director's, and Under Secretary's comments were responsive, and no additional comments are required.

A.6. We recommend that the Director, Defense Manpower Data Center add a notification screen in the Contractor Verification System that, at a minimum, informs applicants about section 701, title 18, United States Code and explains that revoked Common Access Cards must be returned to specific Government personnel as determined in Recommendation A.5.b.(5).

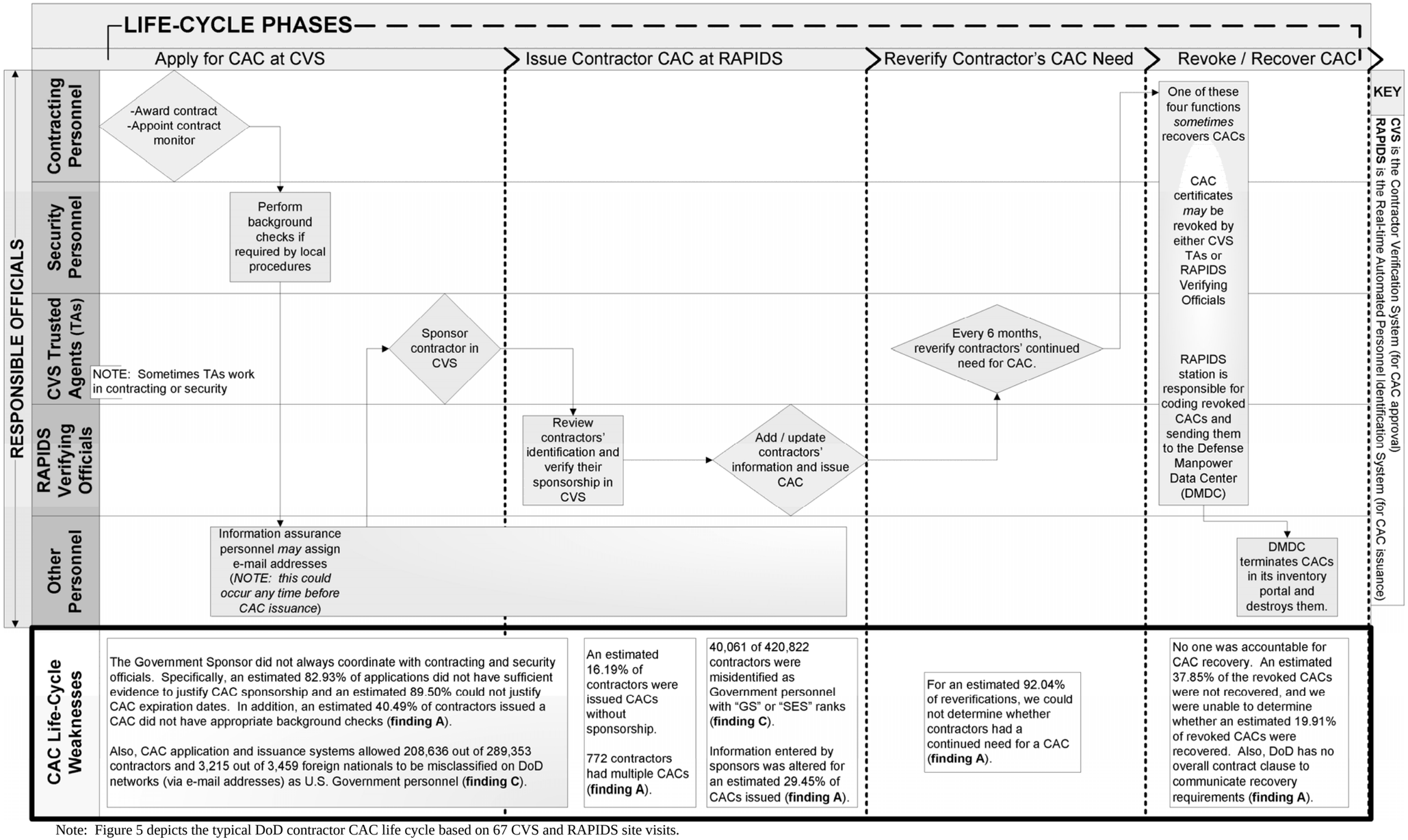
Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the Director, DMDC, agreed, stating that DMDC will implement a CVS notification message during the second quarter of FY 2009 to inform contractor applicants of their

responsibility to return terminated or expired CACs to a RAPIDS facility or to specific Government personnel that will be determined during the course of policy development. The Deputy Under Secretary also stated that the notification message will include a reference to section 701, title 18, United States Code and that this information would be added to the CVS online training and user guide.

Our Response

The Deputy Under Secretary's comments were responsive, and no additional comments are required.



Note: Figure 5 depicts the typical DoD contractor CAC life cycle based on 67 CVS and RAPIDS site visits.

Figure 5. Life Cycle of the DoD Contractor Common Access Card

Finding B. Oversight of Common Access Cards for Contractors Deploying to Southwest Asia

The Army did not verify that Kellogg, Brown, and Root, Inc. (KBR) contractors deploying to Southwest Asia had background checks or Government approval before issuing them CACs, or that CACs were recovered after contractor services ended. These weaknesses pose a potential national security risk because, as of July 19, 2007, as many as 25,428 U.S. and foreign national KBR contractors who deployed in support of Southwest Asia operations may have unauthorized access to DoD resources, installations, and sensitive information worldwide. Better Army oversight and CAC life-cycle procedures are required to minimize this risk.

KBR Deployment Processing Center

KBR has its own Deployment Processing Center in Houston, Texas, which provides training, equipment, and CACs to KBR contractors deploying to Southwest Asia. Figure 7 depicts the KBR CAC life cycle for contractors deploying to Southwest Asia. The CAC issuance process at the KBR Deployment Processing Center occurred as follows.

- KBR hired U.S. or foreign national contractors.

- Kroll Background America, Inc. (hereafter referred to as Kroll), a KBR subcontractor, was hired by KBR to perform background checks on KBR contractors.

- KBR prepared a DD Form 1172-2 for its contractors and notarized photocopies of their passports. KBR sent this information to a contractor at Fort Belvoir, Virginia.

- A contractor working with Army Materiel Command (AMC) at Fort Belvoir, Virginia, reviewed the DD Forms 1172-2 and the notarized passport photocopies. If no errors were detected, the contractor distributed the DD Forms 1172-2 to Government officials for signature and then sent the signed forms back to the KBR Deployment Processing Center.

- SI International, Inc. (SI International) a contractor at the KBR Deployment Processing Center, used RAPIDS to issue CACs to KBR contractors based on their signed DD Forms 1172-2.

AMC and the Deputy Under Secretary of the Army for Business Transformation (DUSA-BT) are responsible for monitoring the CAC life cycle at the KBR Deployment Processing Center. Because the KBR contractors were receiving CACs for work under

contract to AMC, AMC was responsible for CAC approval, revocation, and recovery. Both AMC and DUSA-BT were responsible for monitoring CAC issuance at the SI International RAPIDS site. The most recent DUSA-BT contract was awarded in March 2008 for 1 year with an option period for 1 additional year.

Contractor Background

AMC officials had no assurance that KBR contractors received proper background investigations before being issued CACs. AMC officials relied on background investigations performed by Kroll, a KBR subcontractor. However, the subcontractor's criteria for the background investigations performed on KBR contractors did not meet Government requirements for investigations.

As discussed in finding A, Homeland Security Presidential Directive-12 and Federal Information Processing Standard 201-1 require contractors seeking a CAC to have NACI or equivalent investigations (see page 9 for details on background investigation requirements). KBR hired Kroll to perform background investigations for the company's U.S. and foreign national contractors deploying to Southwest Asia. However, the investigations did not meet the requirements of a NACI or equivalent background investigation.[16] Table 4 contrasts NACI requirements with those of the background investigations performed by Kroll for KBR employees.

Table 4. Comparison of Background Investigation Requirements

NACI (Required)	KBR Subcontractor Investigation	
	U.S. Background Check	**Foreign National Check**
Law enforcement records, 5 years	Checks Federal records, criminal records, outstanding warrants for arrest, "Also Known As" records, Social Security number, county records, probation, and pending Court Records	*Not Completed*
FBI name check		*Not Completed*
FBI National Criminal History Fingerprint Check		*Not Completed*
Employment records, 5 years	*Not Completed*	*Not Completed*
Education records, 5 years	*Not Completed*	*Not Completed*
Residential records, 3 years	Address Histories	*Not Completed*
References	*Not Completed*	*Not Completed*
Defense Clearance and Investigations Index	*Not Completed*	*Not Completed*
Security/Suitability Investigations Index	*Not Completed*	*Not Completed*

[16]For our statistical sample analysis in finding A, 27 of 30 contractors were issued their CACs at the KBR Deployment Processing Center without a NACI or equivalent background investigation.

The Kroll background investigations of U.S. contractors were more thorough than those of foreign national contractors, who were required to provide only a 7-year police record from their country of origin. Kroll's only contractual requirement for foreign nationals was to verify that the police record was authentic. Army officials allowed U.S. and foreign national contractors to obtain a CAC without the required background investigation. This practice poses a potential national security risk that may result in unauthorized access to DoD resources, installations, and sensitive information worldwide.

Government Sponsor's Approval

AMC officials do not know whether KBR contractors were properly sponsored before they were issued CACs. Specifically, Government officials sponsoring KBR contractors were geographically removed, requiring these officials to depend on KBR. Additionally, AMC officials allowed the KBR contractors and foreign nationals to use the DD Form 1172-2 instead of the Government mandated CVS to obtain sponsorship for the CAC. Government officials also relied on a contractor to sponsor KBR contractors.

Use of DD Form 1172-2

As of July 2008, KBR contractors deploying to Southwest Asia were not required to apply for a CAC through CVS. Therefore, CVS reverification was bypassed, signifying that the Army had no assurance that KBR contractors had a continued need for CACs (see page 12 for CVS reverification requirements). Instead of using CVS, these contractors applied for their CACs using DD Form 1172-2. According to KBR officials, the company deployed 1,200 to 1,600 contractors per month, making the use of CVS difficult. Considering the number of KBR contractors processed every month, Army CAC program officials agreed that requiring KBR to use CVS would restrict the Army's mission in Southwest Asia. We were unable to obtain any evidence to support these opinions, and there was no official guidance issued by the Army CAC program office for this practice.

The P&R Memorandum required the use of CVS for all contractors and did not authorize the continued use of the DD Form 1172-2. However, AMC officials believed they had a waiver to this policy because they received an e-mail from the DEERS/RAPIDS Project Office, U.S. Army Human Resources Command. This e-mail stated that AMC could continue using DD Form 1172-2 to authorize CAC issuance and that an official waiver from USD (P&R) was not necessary. According to the Office of Inspector General, Office of General Counsel, U.S. Army Human Resources Command had no authority to waive a policy issued by USD (P&R).

KBR Government Sponsors

Government officials located at Fort Belvoir, Virginia, were supposed to sponsor KBR contractors in Houston, Texas, who were applying for CACs. However, a contractor reviewed and was also authorized to approve KBR contractors' DD Forms 1172-2 by comparing them with photocopies of applicants' passports. Verification of background checks, which is normally a Government function, was not performed on KBR contractors prior to approving the contractors' DD Forms 1172-2. According to AMC

officials, the contractor reviewed the DD Forms 1172-2 and placed them on the Government officials' desks for signature. In effect, a contractor was sponsoring contractors, even though, technically, Government officials were signing the DD Forms 1172-2.

Army Oversight of CAC Issuance at the RAPIDS Site Run by SI International

Officials from AMC and the Office of the DUSA-BT did not provide oversight of the RAPIDS CAC issuance site collocated with the KBR Deployment Processing Center in Houston, Texas. This site was operated by SI International, which was awarded a task order by AMC using a DUSA-BT contracting vehicle. The contractor-run RAPIDS site issues CACs to all eligible recipients, but the majority of CAC recipients using this site were KBR contractors deploying to Southwest Asia.

AMC and DUSA-BT relied on contractors to perform contract oversight. Specifically, SI International provided monthly status reports to the contracting officer's representative and functional representative.[17] In these reports, SI International reported its own performance to DUSA-BT, a practice that gave no assurance that contract requirements were being achieved. In addition, prior to March 2008, the functional representative for the contract was a contractor who was not on-site to assess SI International's performance. The task order awarded in March 2008 appointed a Government employee to be the functional representative; however, this individual also was not on-site to assess SI International's performance. See Figure 6 for the current organization of oversight for this contract.

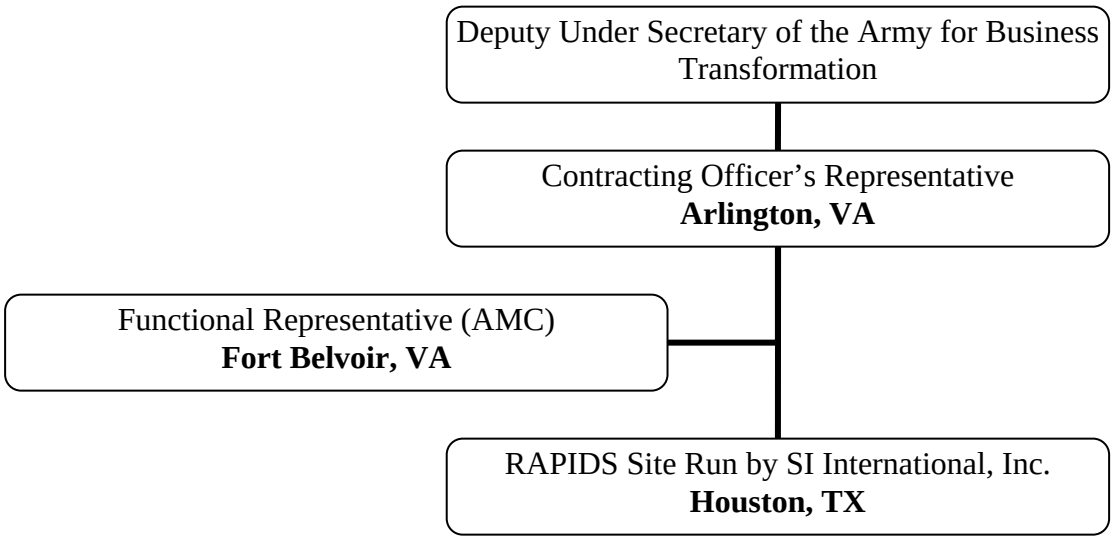


Figure 6. Organization of Oversight for the SI International Contract

[17]DUSA-BT defines the functional representative as the person who serves as the on-site representative to directly observe and assess contractor performance against contract performance standards defined in the contract Performance Requirements Summary.

We tested two of the three contract performance standards in the SI International contract.

- All issued CACs must be accurate, comply with regulatory guidance, and identify the appropriate privileges for each recipient.

- Data entries in RAPIDS must be 100-percent accurate.

Our testing showed that these performance standards were not achieved. Specific deviations included the following.

- CVS was not used to sponsor contractors for CACs.

- Approximately 99 percent of all CACs issued at the site, which were still active as of July 19, 2007, were automatically valid for a 3-year period instead of the contract period of performance.

- Nine out of thirty CACs were issued without sponsorship based on reviewed DD Forms 1172-2.

- RAPIDS Verifying Officials modified information approved on DD Form 1172-2 for 5 out of 30 CACs tested.

To improve performance at the SI International RAPIDS site, the AMC functional representative should assess contractor performance, and DUSA-BT should address the performance assessment with AMC and SI International during the quarterly interim progress reviews as required by the task order. This oversight should occur prior to awarding option periods to SI International for the RAPIDS CAC issuance contract.

CAC Recovery

KBR officials stated that when contractors redeploy to the United States from Southwest Asia, the CACs are collected by KBR and submitted to military officials. However, from January 1 through June 30, 2007, 957 out of 1,966 revoked KBR contractor CACs were not recovered by DoD (48.7 percent). In addition, we could not determine whether DoD recovered 297, or 15.1 percent, of the 1,966 revoked CACs. CAC recovery did not always occur because the CAC and P&R Memoranda did not specify Government officials responsible for collecting revoked CACs. Also, CACs were issued to KBR contractors for 3 years, the maximum period authorized for a CAC. This poses a potential national security risk because if a KBR contractor's CAC was revoked after 1 year[18] but not recovered, the contractor could still use the CAC as a "flash pass" to gain physical access to DoD installations worldwide.

[18]Based on interviews with CVS Trusted Agents, most service contracts are issued for a 1-year period. Therefore, most contractor CACs should be valid for only 1 year.

Conclusion

Army officials did not perform the necessary oversight to verify that KBR contractors deploying to Southwest Asia had authorized access to DoD resources, installations, and sensitive information. AMC officials relied on a KBR subcontractor to perform background investigations of KBR contractors; however, the investigations did not meet Government requirements for CAC issuance. AMC officials also relied on a contractor instead of a Government employee to sponsor KBR contractors, and relied on KBR to recover CACs. Further, AMC officials did not use CVS, which offered better management of contractor CACs than did DD Form 1172-2. Finally, AMC and DUSA-BT relied on SI International to issue CACs to KBR contractors without Government oversight to ensure SI International was complying with contractual requirements. See Figure 7 at the end of this finding for a summary of the contractor CAC life cycle for KBR contractors in Southwest Asia.

A subsequent audit of contractor CACs in Southwest Asia may make additional recommendations about the CAC life cycle for KBR contractors deploying to Southwest Asia.

Client Comments on the Finding and Our Response

Client Comments

The Program Manager, HRsolutions Program Office, responding for the DUSA-BT, provided general comments on the finding. Specifically, the Program Manager stated that the RAPIDS site that SI International operates is housed within the KBR Deployment Processing Center. The Program Manager also stated that eight 3-month option periods were awarded; however, the current contract (awarded in March 2008) was for 1 year with an option period for 1 additional year.

The Program Manager also stated that, although SI International reports its own performance, those monthly performance reports are reviewed and accepted by the Government functional representative and the quality assurance representative in the HRsolutions Program Office. In addition, the Program Manager stated that SI International operates in accordance with a quality control plan specific to its task order, which is approved by the contracting officer's representative and that the functional representative for this site is a Government civilian as are all his office's other (140 or more) functional representatives.

Finally, the Program Manager stated that SI International did not recall issuing CACs to contractors without Government sponsorship, and to SI International's knowledge, all CACs were issued with authorized Government signatures. Further, the Program Manager stated that SI International RAPIDS Verifying Officials did modify information approved on DD Forms 1172-2, for example, by fixing misspellings, but the SI International RAPIDS Verifying Officials did not change pertinent data on entitlements or authorized periods of entitlement.

Our Response

We acknowledge that the RAPIDS site operated by SI International is housed within the KBR Deployment Processing Center. In addition, we updated the finding to clarify that the most recent task order, for SI International's services, was awarded with 1 base year and an option period for 1 additional year.

In addition, we acknowledge that SI International routes its monthly status reports through Government officials; however, the task order states that the Government will evaluate the contractor's performance under the contract in accordance with the performance assessment plan. According to the performance assessment plan, the functional representative is responsible for conducting quarterly visits and assessing contractor performance against contract performance standards. Therefore, the functional representative should have assessed SI International's performance.

We updated the finding to indicate that the functional representative, as of March 2008, was a Government civilian. However, during the audit we obtained evidence that prior to March 2008, the functional representative was a contractor. Also, although SI International does not recall issuing CACs without Government sponsorship, our evidence shows that SI International did issue CACs to contractors without a DD Form 1172-2 and changed authorized periods of entitlement (expiration dates), e-mail certificate privileges, and Geneva Conventions codes.

Recommendations, Client Comments, and Our Response

Revised, Added, and Renumbered Recommendations

As a result of client comments, we revised draft Recommendation B.2. to clarify the nature of the actions needed to monitor the RAPIDS site run by SI International at the KBR Deployment Processing Center. Specifically, Recommendation B.2. was revised to require the functional representative, working for the Logistics Civil Augmentation Program Operations Directorate, to perform contract monitoring functions and to report contractor performance to DUSA-BT. Also, Recommendation B.3. was added to require DUSA-BT to facilitate quarterly interim progress reviews, in accordance with the SI International task order. In addition, draft Recommendation B.3. was renumbered as Recommendation B.4.

B.1. We recommend that the Commander, Army Materiel Command:

a. Mandate use of the Contractor Verification System at the Kellogg, Brown, and Root, Inc. Deployment Processing Center and appoint Government employees to sponsor Kellogg, Brown, and Root, Inc. contractors in the Contractor Verification System in accordance with the Under Secretary of Defense for Personnel and Readiness Memorandum, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005.

Client Comments

The Executive Deputy to the Commanding General, AMC, responding for the Commander, AMC, agreed, stating that AMC will ensure compliance and would use CVS by September 1, 2008.

Our Response

The Executive Deputy's comments were partially responsive. We acknowledge the Executive Deputy's actions to ensure compliance and use CVS by September 1, 2008. However, the Executive Deputy did not address whether Government employees would be appointed to perform TASM and Trusted Agent duties. Therefore, we request that the Commander, AMC, provide comments on the final report by October 31, 2008, addressing the appointment of Government employees to sponsor KBR contractors in CVS.

b. Verify that Kellogg, Brown, and Root, Inc. contractors undergo background checks that meet Homeland Security Presidential Directive-12 and Federal Information Processing Standard 201-1 requirements prior to issuing these contractors Common Access Cards, and maintain evidence of these background checks, (See Recommendation A.5. for additional information.)

Client Comments

The Executive Deputy to the Commanding General, AMC, responding for the Commander, AMC, agreed. The Executive Deputy acknowledged that KBR contractors should undergo background checks and explained procedures that AMC will implement to verify that KBR contractors undergo background checks.

Our Response

The Executive Deputy's comments were partially responsive. We agree that the steps outlined by the Executive Deputy will correct many of the identified weaknesses. However, the Executive Deputy did not provide details regarding what evidence would be maintained for verifying background checks prior to CAC issuance. Therefore, we request that the Commander, AMC, provide comments on the final report by October 31, 2008, that address maintaining appropriate evidence of background checks.

c. Confirm DoD affiliation of contractors before approving their Common Access Card requests, and maintain evidence of such confirmation.

Client Comments

The Executive Deputy to the Commanding General, AMC, responding for the Commander, AMC, agreed. The Executive Deputy explained procedures that AMC will implement to confirm the contractors' affiliation with DoD before approving their CACs and stated AMC will maintain a file of such information.

Our Response

The Executive Deputy's comments were responsive, and no additional comments are required.

d. Implement procedures to recover Common Access Cards from Kellogg, Brown, and Root, Inc. contractors when the cards are expired or no longer needed.

Client Comments

The Executive Deputy to the Commanding General, AMC, responding for the Commander, AMC, agreed. The Executive Deputy explained procedures that AMC will implement to recover contractor-issued CACs.

Our Response

The Executive Deputy's comments were responsive, and no additional comments are required.

B.2. We recommend that the Commander, Army Materiel Command require the functional representative to conduct site visits to the SI International Real-time Automated Personnel Identification System site at the Kellogg, Brown, and Root, Inc. Deployment Processing Center to assess contractor performance, in accordance with the task order, and to provide the results of the performance assessment to the Office of the Deputy Under Secretary of the Army for Business Transformation during the quarterly interim progress reviews required by the task order.

Client Comments

The Program Manager, HRsolutions Program Office, responding for DUSA-BT, disagreed, stating that the HRsolutions Program Office was not staffed to assign personnel to monitor work at all of its customers' sites. The Program Manager stated that the HRsolutions Program Office monitors task order performance through interim reviews, monthly reports, the quality control plan, and dialogue with the contracting officer's representative.

The Program Manager stated that AMC used a DUSA-BT contract to purchase a requirement that was awarded by the Army's Contracting Center of Excellence. The Program Manager stated that, in accordance with the task order, the functional representative is tasked with conducting quarterly visits and assessing contractor performance against contract performance standards. The Program Manager further stated that the contracting officer's representative employed by DUSA-BT is responsible for execution and oversight.

The Program Manager acknowledged that no contracting officer's representative or other Government employee was on site at the RAPIDS facility within the KBR Deployment Processing Center. However, the Program Manager stated that in the past, AMC

Logistics Civil Augmentation Program employees visited the KBR Deployment Processing Center to perform oversight and ensure security requirements were met. The Program Manager also stated that AMC relied on Defense Contract Management Agency employees in the Houston area to visit the SI International RAPIDS site within the KBR Deployment Processing Center when a Government presence was required. Further, the Program Manager stated that monthly reports from the contractor, SI International, indicate that the site was in compliance with contractual requirements.

The Program Manager recommended that AMC continue to make quarterly site visits to the SI International RAPIDS site to monitor the CAC process, and stated that DUSA-BT would continue to monitor the SI International task order in the same manner as his office did the other 140 or more task orders.

Our Response

The Program Manager's comments were partially responsive. We acknowledge that AMC, as the customer, should assess the contractor's performance, but we also recognize that DUSA-BT is ultimately responsible for contract execution and oversight and should facilitate quarterly progress reviews to ensure that appropriate performance monitoring occurs. Although SI International's monthly status reports indicate that performance standards were met, these reports were written by the contractor assessing its own performance. Therefore, we revised Recommendation B.2. to require the functional representative, working for the Logistics Civil Augmentation Program Operations Directorate, to perform contract monitoring functions and report contractor performance to DUSA-BT, in accordance with the task order. In addition, we added Recommendation B.3. to require DUSA-BT to facilitate quarterly progress reviews, in accordance with the SI International task order. We request that the Commander, AMC, review the revised recommendation and provide comments on the final report by October 31, 2008.

B.3. We recommend that the Deputy Under Secretary of the Army for Business Transformation facilitate quarterly progress reviews of the Common Access Card issuance site run by SI International with representatives from the Army Materiel Command, as required in the SI International task order, and maintain evidence of what occurred during these reviews in the official contract file.

Client Comments

See the discussion under Recommendation B.2.

Our Response

As a result of comments from the Program Manager, HRsolutions Program Office, we added Recommendation B.3. to require DUSA-BT to facilitate quarterly progress reviews, in accordance with the SI International task order. Therefore, we request that DUSA-BT review the added recommendation and provide comments on the final report by October 31, 2008.

B.4. We recommend that the Adjutant General, U.S. Army Human Resources Command inform the U.S. Army Defense Enrollment Eligibility and Reporting System / Real-time Automated Personnel Identification System Project Office that it is not permitted to waive DoD policy unless explicitly delegated that authority.

Client Comments

The Adjutant General, U.S. Army Human Resources Command agreed, stating that corrective action has been taken to ensure that the Army DEERS/RAPIDS project office complies with DoD identity card issuance policies and procedures. The Adjutant General also stated that the Army DEERS/RAPIDS Project Office has been notified that any deviation from DoD policy will not occur without prior coordination and approval from the Office of the Secretary of Defense.

Our Response

The Adjutant General's comments were responsive, and no additional comments are required.

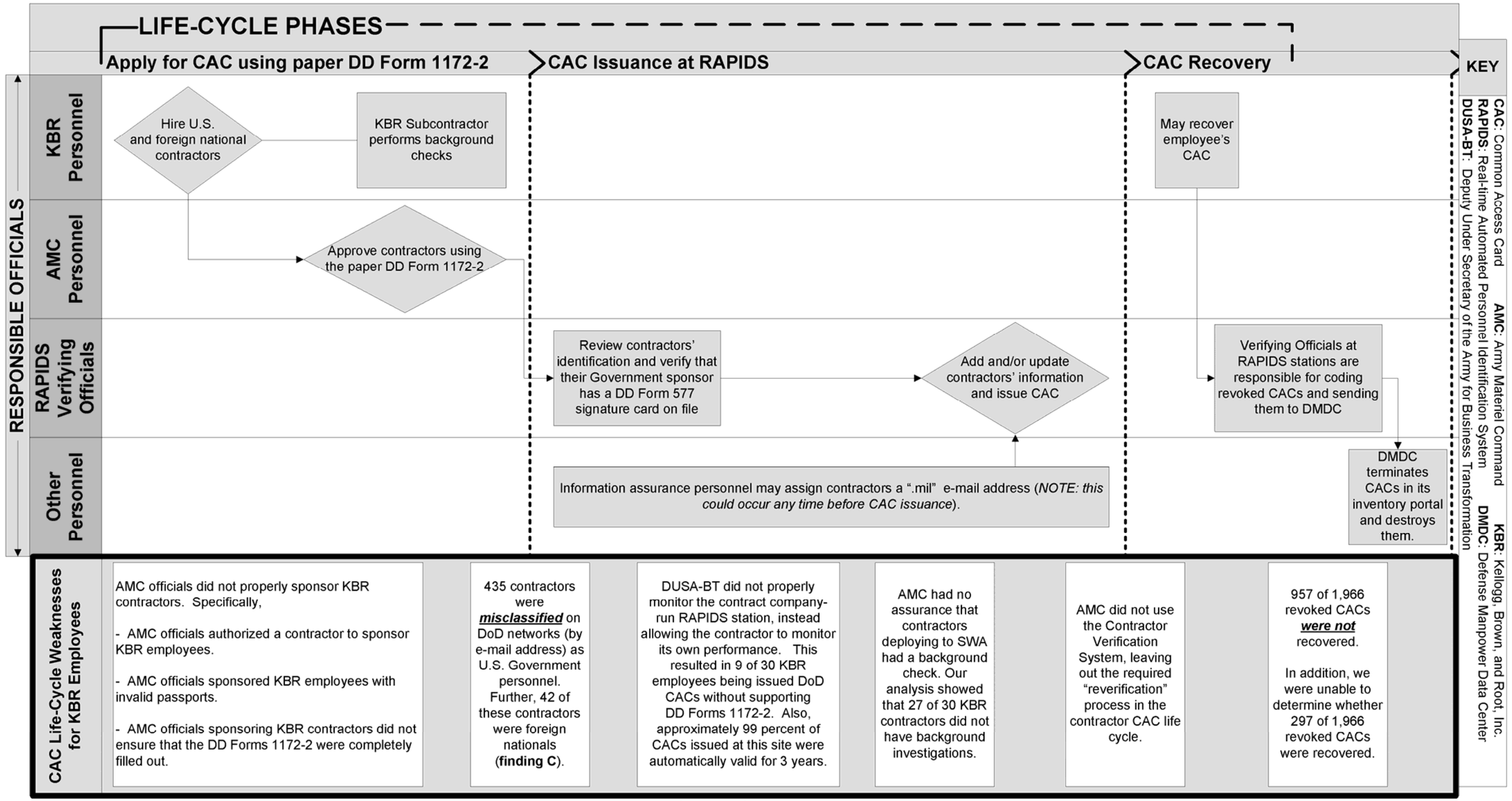


Figure 7. CAC Life Cycle for KBR Contractors Deploying SWA

Finding C. Identification of U.S. and Foreign National Contractors

U.S. and foreign national contractors with CACs were misidentified as U.S. Government personnel. Specifically, DMDC data indicated that:

- 40,055 out of 420,822 contractor CACs indicated their holders had General Schedule (GS) pay grades and were Government personnel; and

- 208,636 out of 289,352 U.S. contractors and 3,215 out of 3,459 foreign national contractors with CAC e-mail signature and encryption certificates had e-mail addresses identifying them as U.S. Government personnel.

This misidentification poses a potential national security risk because U.S. and foreign national contractors could misrepresent themselves both in person and on DoD networks to improperly obtain sensitive information or Government privileges worldwide. USD (P&R) should implement additional system controls for CVS and RAPIDS to prevent misidentification of contractors.

Classification of U.S. Government Personnel

In general, the CACs of civilians and contractors are assigned one of four personnel classifications: GS, Senior Executive Service (SES), GS-Equivalent, or Other. Both GS and SES classifications represent pay grades for Federal civilian employees, while GS-Equivalent or Other are reserved for contractors.

Pay Grade

Out of 420,822 DoD and non-DoD contractors, approximately 9.5 percent, or 40,055, had CACs that were inappropriately assigned GS pay grades. This occurred because RAPIDS does not include controls to limit pay grade entries to GS-Equivalent or Other for U.S. and foreign national contractors. In addition, the CVS application, which must be approved before CAC issuance, does not include sections that would allow Trusted Agents to:

- identify the pay grade of U.S. and foreign national contractors as GS-Equivalent or Other, or

- distinguish the U.S. and foreign national contractors who require a Geneva Conventions CAC (defined on the following page).

Because of these limitations, RAPIDS Verifying Officials enter the pay grades and Geneva Conventions code based on contractors' deployment documents. As a result, contractors with inappropriate pay grades on their CACs could obtain sensitive information and benefits such as housing and transportation that are available only to U.S. Government personnel. Additionally, contractors inappropriately classified as a

senior civilian Government employee could be given higher priority for transport in theaters of combat, affecting the combatant Commander's priorities. This mistaken precedence could further affect the Commander's priorities in supporting the warfighter. Table 5 provides details for the contractor CACs with inappropriate GS pay grades.

Table 5. Contractors With Inappropriate GS CACs

Pay Grade	Number of Contractors
GS-01	691
GS-02	127
GS-03	236
GS-04	773
GS-05	2,588
GS-06	1,043
GS-07	1,608
GS-08	986
GS-09	2,963
GS-10	1,405
GS-11	3,307
GS-12	12,354
GS-13	6,670
GS-14	2,856
GS-15	2,448
TOTAL	**40,055**

In addition, we identified 6 out of 420,822 contractors who were assigned SES pay grades on their CACs. Although this misclassification did not occur often, RAPIDS should be modified to disallow both GS and SES pay grades for contractors.

Geneva Conventions CAC

Of the 40,061 contractor CACs that were inappropriately assigned GS or SES pay grades, 40,055 were Geneva Conventions CACs. Contractors are not required to have GS or SES pay grades to obtain a Geneva Conventions CAC; instead, contractors should be assigned the pay grade "Other" to prevent contractors from being misidentified as Government personnel.

The Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces, referred to as a Geneva Conventions CAC, differs from other types of CACs. Specifically, Geneva Conventions CACs are issued to civilians and contractors who accompany the Armed Forces during a conflict, combat, or contingency operation. Civilians and contractors use the Geneva Conventions CAC to receive commissary, exchange, morale, welfare, and recreation benefits and medical privileges while they accompany the Armed Forces.

The Geneva Conventions CAC looks like other CACs; however, there is no green stripe to identify contractors, and the bearer's pay grade is printed on the front of the card.

Figure 8 shows a Geneva Conventions CAC and details the items printed on the front and back of the card. Figure 9 shows a contractor or foreign national CAC for comparison.

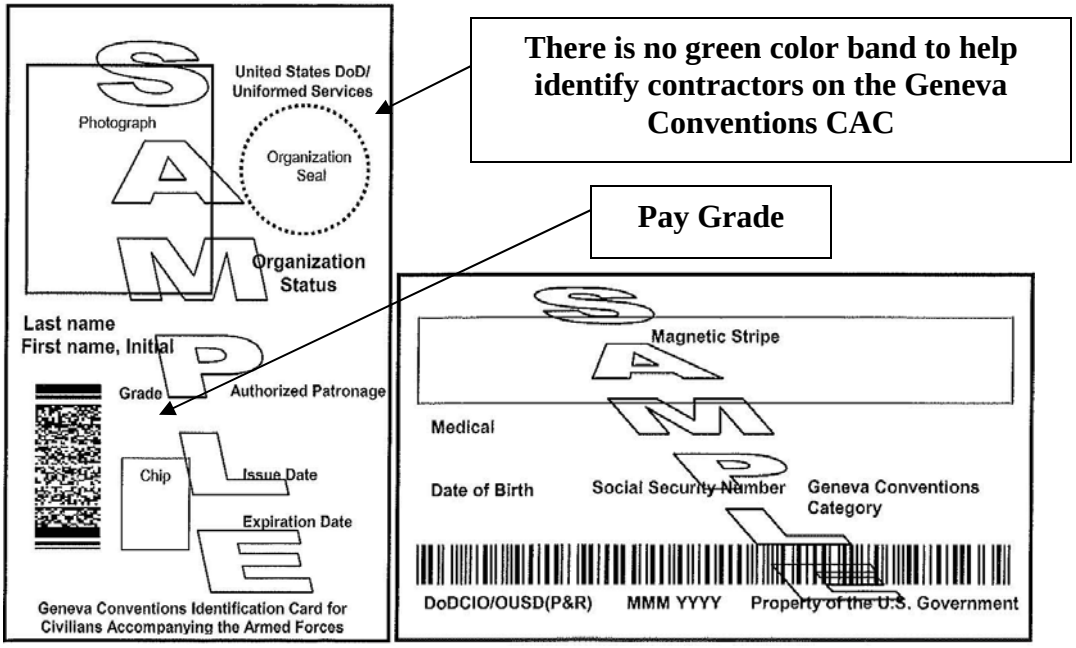


Figure 8. Geneva Conventions CAC for Contractors

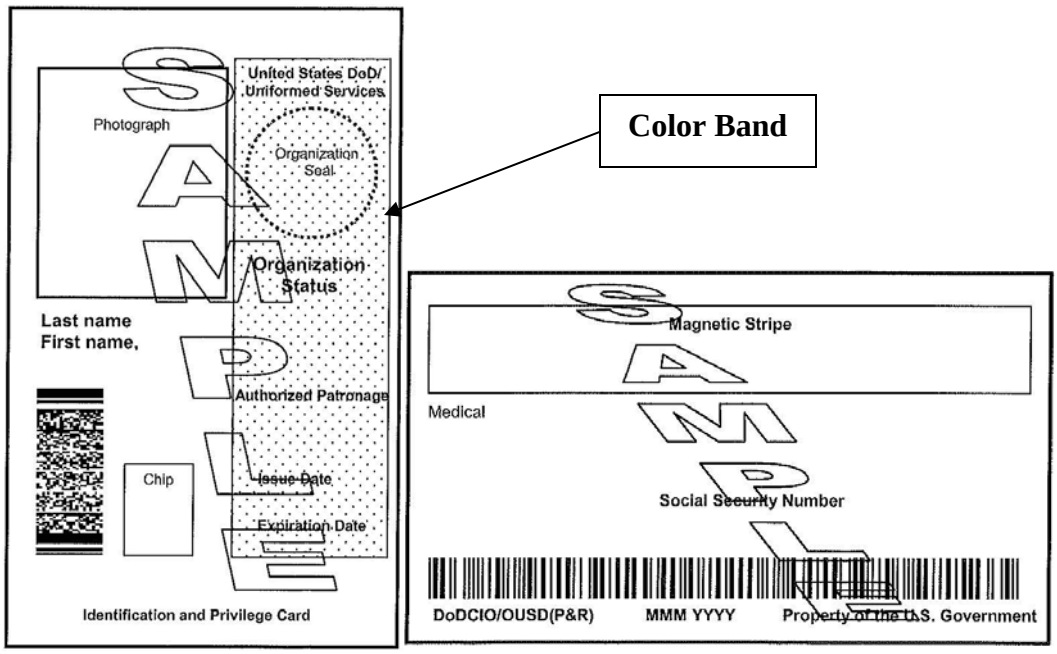


Figure 9. CAC With Color Band for Contractors and Foreign Nationals

Trusted Agents are more suitable for entering pay grade and Geneva Conventions code because, as the sponsors, they have more knowledge than Verifying Officials of contractors' information and need for CACs. Additionally, some Trusted Agents were also DoD contracting personnel. Therefore, Trusted Agents were familiar with contract

scope and work requirements. If Trusted Agents were responsible for entering pay grades and Geneva Conventions codes in CVS, and if those fields were blocked in RAPIDS, Verifying Officials would be unable to modify the data.

E-mail Addresses

DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, requires all systems that process sensitive information to have a control called "affiliation display." Affiliation display requires contractors to have ".ctr" in their e-mail addresses, and foreign national contractors to have their two-digit country code in their e-mail addresses. Table 6 provides examples of proper contractor and foreign national e-mail addresses, display names, and automated signature blocks, based on DoD Instruction 8500.2.

Table 6. Appropriate Contractor and Foreign National E-mail Identifiers*

Affiliation Display	Examples
DoD user e-mail address	john.smith.ctr@army.mil or john.smith.uk@army.mil or john.smith.ctr.uk@army.mil**
DoD user e-mail display name	John Smith, Contractor, john.smith.ctr@army.mil; or John Smith, United Kingdom, john.smith.uk@army.mil
Automated signature block	John Smith, Contractor, J-6K, Joint Staff or John Smith, United Kingdom, J-6K, Joint Staff

*Our primary focus was on the ".mil" and ".ctr" e-mail address identifiers.
** The e-mail identifies contractors who are also foreign nationals.

E-mail addresses for 208,636 out of 289,352 U.S. contractors and 3,215 out of 3,459 foreign national contractors misclassified them as U.S. Government personnel.[19] Specifically, contractors' e-mail addresses were written in the same format as U.S. Government personnel rather than a format identifying them as being either U.S. or foreign national contractors. Misclassification occurred because information assurance personnel did not establish e-mail addresses for U.S. and foreign national contractors in accordance with DoD Instruction 8500.2. Also, CVS and RAPIDS were not designed to reject the incorrect e-mail addresses.

Furthermore, Verifying Officials stated that they granted U.S. and foreign national contractors logical access to DoD networks if the contractors were able to provide a ".mil" e-mail address. Because the Verifying Official does not sponsor the contractor, it would be more appropriate for the CVS Trusted Agent to determine whether contractors

[19]Based on the active CAC data obtained from DMDC, all of these contractors had three Public Key Infrastructure certificates on their CACs. These certificates, among other things, are used to validate an individual's identity and right to send and receive sensitive information through DoD Web sites and military (.mil) e-mail addresses.

require logical access to sensitive DoD networks. However, CVS did not require Trusted Agents to make this determination.

Conclusion

DMDC data indicated that RAPIDS did not have controls to limit pay grade entries, and CVS did not have a field for identifying U.S. and foreign national contractors as either GS-Equivalent or Other. In addition, neither system was designed to reject contractors' e-mail addresses if they lacked the ".ctr" identifier. As a result, U.S. and foreign national contractors' CAC applications were approved in CVS even though their e-mail addresses lacked proper identifiers, and U.S. and foreign national contractors were issued CACs with pay grades that misidentified them as U.S. Government employees. Both the misclassification of pay grades and inappropriate e-mail addresses increase potential risks to national security in the following ways.

- DoD military and civilian personnel may inadvertently disclose controlled or sensitive information to U.S. and foreign national contractors.

- U.S. and foreign national contractors may misrepresent themselves to gain physical and logical access to DoD facilities, resources, and information.

- U.S. and foreign national contractors may be able to obtain transportation and other support before military personnel in theater, affecting Commanders' priorities in supporting the warfighter.

- U.S. and foreign national contractors could evade DoD oversight.

These risks would be minimized if pay grades and Geneva Conventions codes were assigned in CVS by a Trusted Agent, and if RAPIDS had controls to prevent changes to these fields. Furthermore, risks would be minimized if Trusted Agents recorded their determination of contractors' needs for logical access and required appropriate e-mail addresses before approving CAC applications. USD (P&R) could effect these changes by implementing a CAC recovery plan and adequate system controls.

Actions Taken by the Defense Manpower Data Center

After we received the Under Secretary of Defense for Program Integration's comments on the draft audit report, we received additional comments from the DMDC Chief, Operations-Personnel Identity Protection Solutions Division. The DMDC Chief stated that USD (P&R) will implement a "pop-up" screen to inform and remind CVS users that contractors' e-mail addresses should include a ".ctr" identifier. The DMDC Chief also stated that USD (P&R) will release this CVS update during the second quarter of FY 2009.

Recommendations, Client Comments, and Our Response

Revised Recommendation

As a result of client comments, we revised draft Recommendation C.1.c. to clarify the need to add a field in CVS for Trusted Agents to document a contractor's need for Public Key Infrastructure digital certificates.

C.1. We recommend that the Under Secretary of Defense for Personnel and Readiness develop and implement the following system controls in the Contractor Verification System and the Real-time Automated Personnel Identification System:

a. Classify contractor pay grade as "Other" and reject incorrect e-mail addresses, as specified in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 3, 2003, for U.S. and foreign national contractors in the Contractor Verification System.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), partially agreed with implementing system controls to classify pay grades, but disagreed with implementing system controls to reject incorrect e-mail addresses. Specifically, the Deputy Under Secretary stated that the USD (P&R) agrees that inappropriate categorization in the pay grade field needs to be addressed for contractors eligible for the Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces. The Deputy Under Secretary explained that RAPIDS, rather than CVS, requires a pay grade to designate an equivalent Geneva Convention code category in accordance with DoD Instruction 1000.1, "Identity Cards Required by the Geneva Conventions," at the time of CAC issuance, and that classifying contractor pay grade as "OTHER" in RAPIDS would still require a method to determine the appropriate Geneva Conventions code category. As a solution, the Deputy Under Secretary proposed that, by the end of 2008, DMDC modify RAPIDS to allow Verifying Officials to continue to enter the pay grade for contractors needing Geneva Conventions Identification Cards, but the printed face of all contractor CACs would display only "OTHER" for the pay grade.

As for implementing system controls that reject incorrect e-mail addresses, the Deputy Under Secretary stated that e-mail addresses for CAC holders are stored within the DoD Public Key Infrastructure e-mail signing and e-mail encryption certificates. The Deputy Under Secretary further stated that these fields have no technical function in CAC Public Key Infrastructure-based Web site authentication, network authentication, e-mail signing, or e-mail encrypting. The Deputy Under Secretary determined that, because the requirement in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, to designate contractors and foreign nationals is assigned to the network administrators who establish and manage network and e-mail accounts, enforcing the rejection of incorrect e-mail addresses within the CAC issuance process

would not limit any system risk associated with the naming convention of network and e-mail accounts.

Our Response

The Deputy Under Secretary's comments were partially responsive. We agree with the proposed action for DMDC to modify RAPIDS by the end of 2008 so that the printed face of all contractor CACs will display only "OTHER" for the pay grade. However, we disagree that the requirement in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, to designate contractors and foreign nationals is assigned to the network administrators who establish and manage network and e-mail accounts. Specifically, DoD Instruction 8500.2 requires the heads of the DoD Components, including the USD (P&R), to ensure that DoD information systems acquire and employ information assurance solutions. These solutions include the control of "affiliation display," which requires contractors to have ".ctr" in their e-mail addresses and foreign national contractors to have their two-digit country code in their e-mail addresses. Therefore, we request that the USD (P&R) reconsider his position on Recommendation C.1.a. regarding rejecting incorrect e-mail addresses in CVS and provide comments on the final report by October 31, 2008.

b. Lock the pay grade field for contractors and reject incorrect e-mail addresses, as specified in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 3, 2003, for U.S. and foreign national contractors in the Real-time Automated Personnel Identification System.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), partially agreed and referred to the comments in response to Recommendation C.1.a.

Our Response

The Deputy Under Secretary's comments were partially responsive. We agree with the proposed action for DMDC to modify RAPIDS by the end of 2008 so that the printed face of all contractor CACs will display only "OTHER" for the pay grade. However, we disagree that the requirement in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, to designate contractors and foreign nationals is assigned to the network administrators who establish and manage network and e-mail accounts. Specifically, DoD Instruction 8500.2 requires the heads of DoD Components, including the USD (P&R), to ensure that DoD information systems acquire and employ information assurance solutions. These solutions include the control of "affiliation display," which requires contractors to have ".ctr" in their e-mail addresses and foreign national contractors to have their two-digit country code in their e-mail addresses. Therefore, we request that the USD (P&R) reconsider his position on Recommendation C.1.b. regarding rejecting incorrect e-mail addresses in RAPIDS, and provide comments on the final report by October 31, 2008.

c. Add a field in the Contractor Verification System for Trusted Agents to document a contractor's need for Public Key Infrastructure digital certificates.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), disagreed, stating that, in coordination with the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer and during the DoD instruction development process, CAC holders' eligibility for network access probably will be defined in greater detail. Furthermore, the Deputy Under Secretary stated that determination of eligibility for network logon and the management of network accounts may not necessarily rest with the CVS Trusted Agents, but with others in their organization, leaving the value added, practicality, and enforceability of capturing this information in CVS unclear.

Our Response

We concluded from the Deputy Under Secretary's response that our recommendation was unclear. We revised the recommendation to clarify the need to add a field in CVS for Trusted Agents to document a contractor's need for Public Key Infrastructure digital certificates. Therefore, we request that the USD (P&R) review the revised recommendation and provide comments on the final report by October 31, 2008.

C.2. We recommend that the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer:

a. Designate within 90 days the lead organization responsible for immediately developing and implementing a recovery plan for contractor Common Access Cards showing improper pay grades and e-mail addresses.

b. Implement the recovery plan for contractor Common Access Cards showing improper pay grades and e-mail addresses.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), disagreed. The Deputy Under Secretary stated that the USD (P&R) recognizes that the current CAC infrastructure does not prevent a potentially incorrect or misleading pay grade equivalent from being printed on a contractor's CAC, but this would be corrected. However, the Deputy Under Secretary stated that designating a lead and implementing a recovery plan for CACs that are currently in circulation are out of proportion to the perceived risks cited in the draft report. The Deputy Under Secretary stated specifically that a contractor Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces CAC will still indicate that the individual is a "Contractor" or "Foreign Affiliate" even if the card displays an incorrect pay grade.

Further, the Deputy Under Secretary stated that there was no evidence in the draft report showing that a pay grade on a contractor's card was used to authorize any type of access or privileges. Furthermore, the Deputy Under Secretary stated that there are significant cost implications and operational effects associated with recovering all CACs containing incorrect pay grades and e-mail addresses. Therefore, the Deputy Under Secretary concluded that a more appropriate approach would be to let current CACs be revoked and expire in accordance with the normal life cycle and focus on improving the proper pay grade categorizations for new contractor CACs.

The Under Secretary of Defense for Intelligence agreed, stating that inaccurate information on contractor CACs poses a security threat and likely may affect accreditation of the system under the Privacy Act of 1974. The Under Secretary also stated that the Federal credential uses the red color bar to identify First Responders, and that the color bar on contractor CACs, coupled with inaccurate Government civilian pay grades, poses a significant vulnerability to Federal facilities worldwide.

The Deputy Assistant Secretary of Defense (Information and Identity Assurance), responding for the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, partially agreed. The Deputy Assistant Secretary stated that contractor e-mail addresses are not displayed on the outside of contractor CACs, but appear only in the signing or encryption certificates. The Deputy Assistant Secretary explained that, because use of the card for physical access does not provide access to or expose the e-mail address of the card holder, the number of contractor CACs used in Southwest Asia to authenticate the card holders' eligibility for access to logical resources is very small and poses little risk to DoD operations. However, the Deputy Assistant Secretary stated that the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer intends to work closely with the USD (P&R) and the Under Secretary of Defense for Intelligence to develop a plan focused on immediate recovery and reissuance of CACs with improper e-mail addresses for contractors located in the United States, while improperly issued contractor CACs currently in use in Southwest Asia will be recovered as they expire. The Deputy Assistant Secretary acknowledged that, although recovery and reissuance are important, the immediate focus should be on correcting issuance procedures.

Our Response

The Deputy Under Secretary's, Under Secretary's, and Deputy Assistant Secretary's comments were partially responsive. All three clients acknowledged that recovery and reissuance of CACs are important, and the Deputy Under Secretary and Deputy Assistant Secretary specifically proposed revoking and recovering contractor CACs as they expire. While we agree that this recovery plan will be the least costly and onerous to the Department, we still believe that a lead organization should be designated to coordinate the further development of this recovery plan, and coordination should occur among the three organizations to ensure implementation of the recovery plan. Therefore, we request that the USD (P&R), the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information

Officer reconsider their positions on Recommendations C.2.a. and C.2.b. and provide comments on the final report by October 31, 2008.

Finding D. Oversight of Common Access Card Sponsors

DoD CVS Service Points of Contact (SPOCs) did not fulfill their oversight responsibilities for appointing CAC sponsors[20] and deactivating their accounts. DMDC data indicated that 303 CAC sponsors were contractors, and 45 active CVS CAC application sites had no manager for their sponsors. As a result, contractors and sponsors who left Government service may have been approving CACs. To strengthen oversight of CAC sponsors, DoD should implement procedures to:

- verify that CAC sponsors are Government employees,
- verify that each CVS site has managers, and
- confirm periodically that sponsors should still have authorization to approve contractor CACs.

Organization of CAC Application Sites

Each Service agency has an SPOC who is responsible for coordinating with DMDC to establish and manage CVS sites and Trusted Agent Security Managers (TASMs). Each site may have no more than two TASMs but is allowed unlimited Trusted Agents. The DMDC CVS User's Guide states that TASMs are responsible for appointing and managing Trusted Agents, and that neither TASMs nor Trusted Agents shall be contractors. In addition, a TASM may perform all Trusted Agent functions—for example, sponsoring contractors for CACs. Figure 10 shows how a CVS site should be organized according to the DMDC CVS User's Guide.

[20]CAC sponsors are Trusted Agent Security Managers or Trusted Agents.

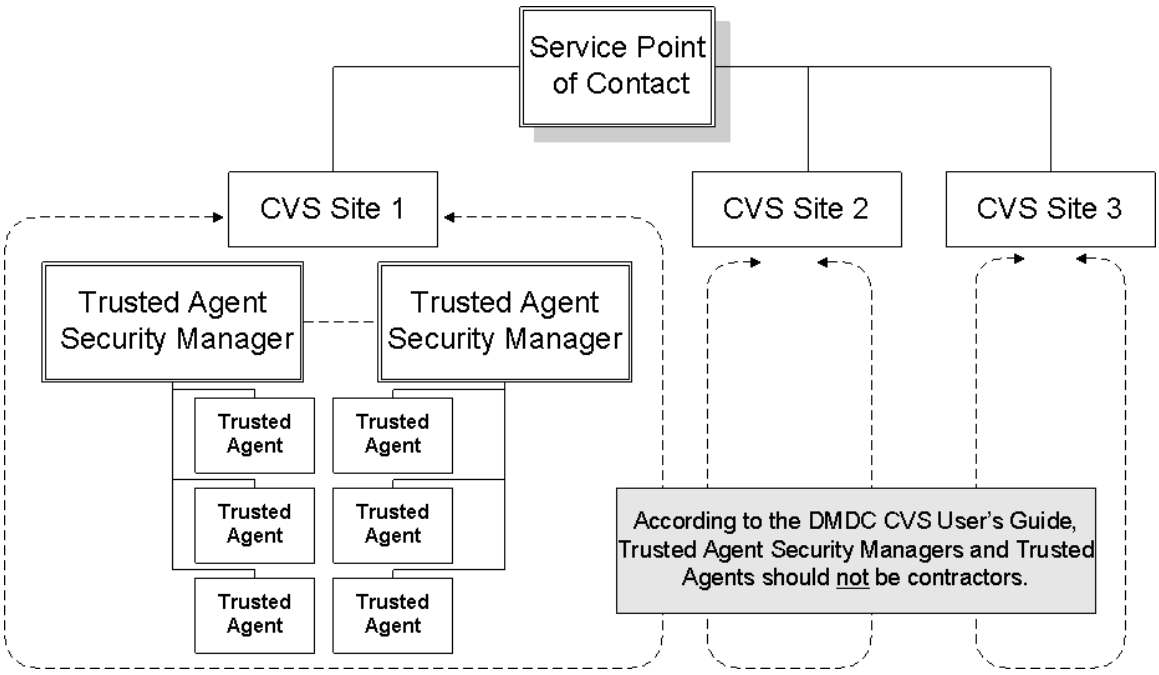


Figure 10. Organization of CVS Sites

Appointment of CAC Sponsors

DMDC data indicated that 303 TASMs and Trusted Agents were contractors.[21] These sponsors managed 1,291 CVS applications during the first 6 months of 2007. Table 7 delineates the classification of CAC sponsors.

Table 7. CAC Sponsors by Personnel Classification

Classification in DEERS	TASMs	Trusted Agents	Total
Contractor with active CAC	22	181	203
Contractor with active CAC who was also in the revoked CAC data we obtained	6	35	41
Contractor with revoked CAC	6	41	47
Not in DEERS as a contractor, but has a ".ctr" e-mail address	4	8	12
Total	**38**	**265**	**303**

According to the DMDC CVS User's Guide, SPOCs establish CVS sites and appoint TASMs by sending a digitally signed e-mail to the DMDC Support Office requesting new or additional CVS capability. Then, the DMDC Support Office generates the TASM record in a system called DEERS Security Online. DEERS Security Online is an

[21]DMDC data indicated that 94 of the 303 TASM and Trusted Agent contractors worked at DMDC Support Centers and testing sites. In addition, 3 TASM and Trusted Agent contractors had no CVS site number and 4 appeared to have accounts that were deactivated, leaving 202 TASM and Trusted Agent contractors working at other CVS sites.

application, separate from CVS, used to authorize TASMs and Trusted Agents to perform their duties.

TASMs also use DEERS Security Online to appoint Trusted Agents. According to DMDC officials, DEERS Security Online does not prevent contractors from becoming Trusted Agents. Rather, DMDC relied on TASMs to ensure that Trusted Agents were not contractors.

Monitoring and Deactivation of CAC Sponsor Accounts

DMDC data indicated that 45 CVS sites had no TASM to manage Trusted Agents. Trusted Agents at these unmanaged sites processed 2,080 CVS applications during the first 6 months of 2007. DMDC officials stated that the data showed some sites appeared to have no TASMs because the TASMs may never have logged in to CVS, or their use of CVS was suspended because of inactivity. Without a TASM, Trusted Agents who left Government service could not have had their accounts deactivated in CVS. According to DMDC data, the accounts of only 10 out of 2,033 TASMs and 10 out of 8,627 Trusted Agents have been deactivated since DoD started using CVS in 2006.

The DMDC CVS User's Guide states that SPOCs are responsible for working with the DMDC Security Team to register, appoint, and remove TASMs. It was unclear how SPOCs accounted for TASMs at each CVS site under their Service or agency. Additionally, the DMDC CVS User's Guide did not include instructions telling TASMs to remove a Trusted Agent who no longer needed access to CVS.

Conclusion

DMDC data indicated that CACs could be approved by contractors and by sponsors who have left Government service. This increases the risk of unauthorized access to Government facilities and information. This risk could be minimized by improving system controls and increasing SPOC and TASM oversight to strengthen the process for appointing TASMs and Trusted Agents and deactivating their CVS accounts.

Actions Taken by the Defense Manpower Data Center

DMDC officials stated that they intended to conduct a self-audit to determine whether TASMs and Trusted Agents were contractors, and, if so, to alert SPOCs to take action. In addition, DMDC officials confirmed that TASMs and Trusted Agents must be Government personnel and stated that they communicated this requirement to SPOCs.

At the end of April 2008, DMDC and the Services started an internal review of Trusted Agents who were contractors. DMDC stated that the Services disabled CVS accounts of Trusted Agents who were contractors. On September 23, 2008, DMDC officials estimated that they would complete this action by November 2008.

Recommendations, Client Comments, and Our Response

D.1. We recommend that the Director, Defense Manpower Data Center:

a. Develop and implement procedures to:

(1) Verify that Trusted Agent Security Managers and Trusted Agents are Government employees before authorizing sponsorship duties.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the Director, DMDC, agreed, stating that DMDC will implement procedures through the Security Online System to verify that a TASM or Trusted Agent is a Government employee or military member. In addition, the Deputy Under Secretary stated that, until a new release of the Security Online System is available, DMDC will provide reports to CVS SPOCs to review and determine the appropriate corrective action for those identified to be inappropriately designated as TASMs and Trusted Agents.

Our Response

The Deputy Under Secretary's comments were responsive, and no additional comments are required.

(2) Verify that Contractor Verification System sites have active Trusted Agent Security Managers.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the Director, DMDC, agreed, stating that DMDC currently monitors the activity of TASM accounts, and if they are inactive for more than 45 days, the account is automatically suspended; after 60 days, the account is deleted. Additionally, the Deputy Under Secretary stated that to reactivate an account the TASM must contact DMDC. Further, the Deputy Under Secretary stated DMDC notifies the CVS SPOCs when there is a site with an inactive TASM.

Our Response

The Deputy Under Secretary's comments were responsive, and no additional comments are required .

b. Establish a plan with defined milestones to identify and deactivate the Contractor Verification System accounts of all current non-Government Trusted Agent Security Managers and Trusted Agents, and implement this plan.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the Director, DMDC, agreed, stating that DMDC will periodically provide the CVS SPOCs a list of active TASMs and Trusted Agents to review and determine which individuals should not be TASMs or Trusted Agents. After we received the Deputy Under Secretary's official comments, we received additional comments from the DMDC Chief, Operations-Personnel Identity Protection Solutions Division, explaining the four phases involved in deactivating CVS accounts of non-Government TASMs and Trusted Agents. The DMDC Chief stated that Phase Four, requesting Service/Agency compliance with removing non-Government TASMs and Trusted Agents, will be completed by November 2008.

Our Response

The Deputy Under Secretary's and the DMDC Chief's comments were responsive, and no additional comments are required.

D.2. We recommend that the Under Secretary of Defense for Personnel and Readiness; Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Under Secretary of Defense for Intelligence incorporate into the joint Common Access Card policy (see Recommendation A.5.) a requirement for Contractor Verification System Service Points of Contact to confirm periodically that Trusted Agent Security Managers and Trusted Agents are authorized to approve contractor Common Access Cards. The joint policy should state how often the Service Points of Contact should perform this action.

Client Comments

The Deputy Under Secretary of Defense for Program Integration, responding for the USD (P&R), agreed, stating that procedures and processes would be outlined in the DoD instruction referenced in response to Recommendation A.3.e.(1).

The Principal Deputy Director, Acquisition Resources and Analysis, responding for the USD (AT&L), agreed, stating that the USD (AT&L) will work with the USD (P&R) and the Under Secretary of Defense for Intelligence to implement this recommendation.

The Under Secretary of Defense for Intelligence agreed, stating that the staff in the Office of the Secretary of Defense has convened a working group to address Homeland Security Presidential Directive-12 implementation and CAC policy.

Our Response

The Deputy Under Secretary's, Principal Deputy Director's, and Under Secretary's comments were responsive, and no additional comments are required.

Appendix A. Scope and Methodology

We conducted this performance audit from August 2007 through July 2008 in accordance with generally accepted government auditing standards.[1] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We conducted this audit at 32 CVS and 35 RAPIDS sites at the following locations:

- U.S. Army
  - Headquarters, Department of the Army, Arlington, Virginia
  - Fort Belvoir, Virginia
  - Fort Hood, Texas
  - Fort Bragg, North Carolina
  - Fort Monmouth, New Jersey[2]

- U.S. Navy
  - Commander, Navy Region Mid-Atlantic, Norfolk, Virginia
  - Commander, Navy Region Southwest, San Diego, California
  - Naval Station Norfolk, Virginia
  - Naval Station San Diego, California
  - Naval Air Station, Patuxent River, Maryland

- U.S. Air Force
  - Randolph Air Force Base, Texas
  - Lackland Air Force Base, Texas
  - Wright-Patterson Air Force Base, Ohio
  - Edwards Air Force Base, California

- U.S. Marine Corps
  - Marine Corps Base, Quantico, Virginia
  - Marine Corps Base, Camp Lejeune, North Carolina
  - Marine Corps Air Station, New River, North Carolina
  - Marine Corps Air Station, Miramar, California
  - Marine Corps Recruit Depot, San Diego, California

[1]We conducted a research project on contractor CACs from June through August 2007. Some evidence collected for this research project was used to support our audit results.

[2]Interviews with personnel at this site were performed by telephone.

- Other
    - Defense Contract Management Agency, Houston, Texas (KBR Deployment Processing Center)
    - Defense Finance and Accounting Service, Indianapolis, Indiana
    - Department of State, Washington, D.C.[3]

We interviewed CVS SPOCs, TASMs, Trusted Agents, RAPIDS Site Security Managers, and other personnel responsible for the CAC program. We also collected documentation about CVS and RAPIDS procedures as well as information to test these procedures for contractors in our statistical samples. We also interviewed officials from the following:

- Office of the USD (AT&L);
- Office of the USD (P&R), Defense Human Resources Activity;
- Office of the Under Secretary of Defense for Intelligence;
- Office of the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer;
- Army Materiel Command;
- U.S. Army Human Resources Command;
- Office of the Deputy Under Secretary of the Army—Business Transformation
- Director, DMDC; and
- Office of the Director, Defense Procurement and Acquisition Policy;

Finally, we performed work at DMDC-East in Arlington, Virginia, and DMDC-West in Monterey, California. Specifically, we obtained an understanding of the DEERS, RAPIDS, and CVS systems as well as of the data processed and stored within these systems. We also obtained an understanding of how DD Forms 1172-2 were processed by DMDC and collected some of these forms for audit testing. In addition, we obtained several sets of data, from which we drew four statistical samples to perform audit testing. These data sets are explained in the "Use of Computer-Processed Data" section, and the statistical samples are explained in the "Use of Technical Assistance" section.

Review of Internal Controls

We identified material internal control weaknesses in the DoD contractor CAC life cycle as defined by DoD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006. DoD did not have a joint policy that required contractor CACs to be consistently approved, issued, reverified, and revoked and recovered. Further, DoD did not have procedures to oversee and verify CAC sponsors and their managers. In addition, neither CVS nor RAPIDS had automated controls to prevent improper changes to contractor CAC records. Implementing the recommendations in this report should strengthen national security. A copy of this report will be sent to the senior DoD official responsible for internal controls.

---

[3]Department of State Trusted Agents at this location worked for a CVS site managed by the Department of the Army.

Use of Computer-Processed Data

We relied on six sets of computer-processed data from DMDC for this audit:

- CVS applications from January 1 through June 30, 2007;
- CVS reverifications from January 1 through June 30, 2007;
- CVS TASM and TA rosters through July 27, 2007;
- DEERS records of issued CACs that were active as of July 19, 2007;
- DEERS records of revoked CACs from January 1 through June 30, 2007; and
- ILP CAC terminations from January 1 through November 2, 2007.

We used these data to draw four statistical samples that answered seven questions related to the contractor CAC life cycle as follows.

- CVS applications sample
  - How many applicants worked on valid Government contracts?
  - How many applicants were approved to have a CAC for the length of their contract or 3 years, whichever was shorter?

- CVS reverifications sample
  - How many contractors had a continued need to possess a CAC?

- DEERS records of issued CACs
  - For how many contractors was information in DEERS consistent with the information maintained either in CVS or on the DD Form 1172-2?
  - For how many contractors was the issued CAC supported by either a CVS application or the DD Form 1172-2?
  - How many contractors had a completed NACI?

- DEERS records of revoked CACs[4]
  - How many revoked CACs were recovered?

In addition, we used computer-processed data to test the following nonsample questions.

- How many TASMs and TAs were contractors?
- How many TASMs and TAs were deactivated from CVS?
- How many CVS applications were managed by each TASM and TA?
- How many contractors had multiple active CACs?
- How many contractors have Government pay grades on their CACs?
- How many CACs with Government pay grades were Geneva Conventions CACs?

[4]We used ILP CAC termination data to determine whether revoked CACs were recovered.

- How many contractors have ".mil" e-mail addresses and three digital certificates on their CACs to facilitate identification, signing e-mail, and encrypting e-mail?
- How many contractors with a ".mil" e-mail address and three digital certificates on their CACs were identified as contractors in their e-mail addresses, in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003?
- How many contractor CACs were revoked because they were lost?
- How many contractors issued CACs at the KBR Deployment Processing Center were planning to work in Southwest Asia?
- How many revoked contractor CACs, issued at the KBR Deployment Processing Center, were recovered?
- For what length of time were CACs issued at the KBR Deployment Processing Center valid?

The computer-processed data were sufficiently reliable, based on tests performed, given our use of the data previously described. However, we did identify several errors in the computer-processed data, none of which significantly impacted our audit results. To further minimize the impact of errors in the data, we obtained additional written and testimonial evidence during our site visits to support our audit results. The detailed discussion of errors in the computer-processed data sets will be provided on request.

Use of Technical Assistance

The contractor CAC life cycle occurred worldwide across 1,397 CVS sites and 1,474 RAPIDS sites.[5] Due to the scope of this process, we decided to use statistical sampling for the audit. The first step for statistical sampling was to develop subpopulations for the data sets corresponding to the contractor CAC life cycle. These subpopulations were developed by identifying the CVS and RAPIDS locations with the highest levels of activity (i.e., CVS applications managed, reverifications conducted, and CACs issued) for the Services and agencies. Based on the four locations with the most activity for each Service and agency, we determined geographic clusters with 129 CVS and 89 RAPIDS sites which comprised our subpopulations. These subpopulations included Army, Navy, Air Force, Marine Corps, and Defense Agency CVS and RAPIDS sites. The number of records in each subpopulation was as follows:

- 39,532 CVS applications,
- 32,098 CVS reverifications,
- 97,117 issued CACs, and
- 28,205 revoked CACs.

The Office of Inspector General Quantitative Methods Directorate developed the statistical samples of (1) CVS applications, (2) CVS reverifications, (3) CACs issued, and (4) CACs revoked for each audit subpopulation. They used stratified sample design to

[5]The number of CVS and RAPIDS sites includes deployable sites and was based on data obtained in August 2007.

ensure that each of the Services and agencies in our subpopulations were appropriately represented in the samples. The Quantitative Methods Directorate used SAS (Statistical Analysis System) to select appropriate random samples from each stratum. In addition, they performed calculations to make statistically defensible estimates for the subpopulations based on the audited sample results and assisted in interpreting and using the estimates correctly. See Appendix B for detailed information about the work performed by the Quantitative Methods Directorate.

In addition, the Office of Inspector General Personnel Security Office provided JPAS results for each statistically selected issued CAC record. Specifically, Security officials queried JPAS for each individual in the sample by their Social Security number. This information was extracted during November 2007.

Prior and Related Coverage

This audit is the first in a series on the contractor CAC. The second in the series focuses on the contractor CAC in Southwest Asia. The third in the series focuses on the contractor CAC in the Republic of Korea. Subsequent CAC audits may be planned for other overseas locations.

During the last 5 years, the Government Accountability Office, the Department of Defense Inspector General, the Naval Audit Service, and the Air Force Audit Agency have issued seven reports discussing CACs. Unrestricted Government Accountability Office reports can be accessed over the Internet at http://www.gao.gov. Unrestricted Department of Defense Inspector General reports can be accessed at http://www.dodig.mil/audit/reports. Unrestricted Naval Audit Service reports are not available over the Internet. Unrestricted Air Force Audit Agency reports can be accessed over the Internet at http://www.afaa.hq.af.mil/domainck/index.shtml.

Government Accountability Office

Government Accountability Office Report No. GAO-07-525T, "Stabilizing and Rebuilding Iraq: Conditions in Iraq Are Conducive to Fraud, Waste, and Abuse," April 23, 2007

Government Accountability Office Report No. GAO-06-178, "Agencies Face Challenges in Implementing New Federal Employee Identification Standard," February 2006

Department of Defense Inspector General

Department of Defense Inspector General Report No. D-2008-104, "DoD Implementation of Homeland Security Presidential Directive-12," June 23, 2008

Navy

Naval Audit Service Report No. N2005-038, "Common Access Card Implementation," April 8, 2005

Air Force

Air Force Audit Agency Report No. F2008-0005-FD2000, "Controls Over Contractor Identification," April 2, 2008

Air Force Audit Agency Report No. F2007-0018-FCR000, "Common Access Card Use for Physical Access, Headquarters Air Force Reserve Command, Robins Air Force Base, GA," April 27, 2007

Air Force Audit Agency Report No. F2007-0014-FCR000, "Common Access Card Use for Physical Access, 116th Air Control Wing, Robins Air Force Base, GA," April 12, 2007

Appendix B. Estimates Based on Statistical Sampling

We requested estimates from the Office of Inspector General's Quantitative Methods Directorate to answer questions explained in Appendix A in the "Use of Computer-Processed Data" section.[1] In general, these estimates quantified the weaknesses present in each phase of the contractor CAC life cycle. The estimates are based on a 90-percent confidence level. The 90-percent confidence level means there is a 10-percent risk that the interval does not encompass the true subpopulation value.

The statistical estimates are in the table on the next page. The first row in the table shows that between 76.17 percent and 89.68 percent of the 39,532 CVS applications did not have enough evidence to link the applicant to a valid Government contract. The point estimate[2] was 82.93 percent. The corresponding number of CVS applications with insufficient evidence linking the applicant to a valid Government contract lies in a range from 30,113 to 35,451, with a point estimate of 32,782. The other seven estimates can be interpreted the same way.

[1]There were only seven sample questions in Appendix A. The eighth estimate was done to determine the number of revoked CACs for which recovery was undeterminable.

[2]The point estimate is a single numerical value halfway between the upper and lower bounds.

Detailed Statistical Estimates of Weaknesses in Each Phase of the Contractor CAC Life Cycle

Answer to Question in Appendix A	Lower Bound (Percent)	Point Estimate (Percent)	Upper Bound (Percent)	Records in Subpopulation
CVS Applications: Applicants Whose Link to a Valid Government Contract Was Undeterminable	30,113 (76.17)	32,782 (82.93)	35,451 (89.68)	39,532
CVS Applications: Applicants Whose CAC Issuance Length Cannot Be Determined To Be Appropriate	33,332 (84.32)	35,383 (89.50)	37,434 (94.69)	39,532
CVS Reverifications: Contractors Whose Continued Need to Possess a CAC Was Undeterminable	28,054 (87.40)	29,544 (92.04)	31,033 (96.68)	32,098
RAPIDS CACs Issued: Contractors Whose DEERS Record Was Inconsistent With Information in CVS or on DD Form 1172-2	20,918 (21.54)	28,606 (29.45)	36,293 (37.37)	97,117
RAPIDS CACs Issued: Contractors Who Were Issued a CAC Without an Approved CVS Application or DD Form 1172-2	8,973 (9.24)	15,722 (16.19)	22,471 (23.14)	97,117
RAPIDS CACs Issued: Contractors Who Did Not Have a Completed NACI	32,090 (33.04)	39,320 (40.49)	46,550 (47.93)	97,117
RAPIDS CACs Revoked: Contractors Whose Revoked CACs Were Not Recovered	8,570 (30.38)	10,675 (37.85)	12,780 (45.31)	28,205
RAPIDS CACs Revoked: Contractors For Whom Recovery of Revoked CAC Was Undeterminable	3,751 (13.30)	5,615 (19.91)	7,480 (26.52)	28,205

Appendix C. Multiple Active CACs

The table below shows which types of multiple active CACs were held by DoD and non-DoD contractors, based on the computer-processed data we obtained from DMDC. Generally, the meaning for each type of CAC is as follows:

- Identification. This is a regular CAC for physical and, in some cases, logical computer access.
- Identification Privilege. This is an Identification CAC that may have privileges; for example: commissary, morale and welfare, and recreation.
- Accompanying Armed Forces. This is a Geneva Conventions CAC, as described in finding C.
- PIV. Personal Identity Verification CACs are CACs designed for compliance with Homeland Security Presidential Directive-12.

Contractors With Multiple Active CACs

Type of Personnel	Types of CACs	Number of Contractors	Total
DoD Contractor	Identification and Accompanying Armed Forces	13	
	Identification and Identification Privilege	26	
	Identification and PIV Identification	11	
	Identification and Two Identification Privilege	1	
	Identification Privilege and Accompanying Armed Forces	6	
	Two Accompanying Armed Forces	16	
	Two Identification	567	
	Two Identification Privilege	20	**660**
DoD Contractor/ non-DoD Civil Servant	Identification Privilege and Accompanying Armed Forces	5	
	PIV Identification Privilege, and Accompanying Armed Forces	1	
	Identification and Accompanying Armed Forces	3	
	Identification and Identification Privilege	5	
	Two Identification	43	
	Two Identification Privilege	5	**62**
DoD Contractor/ OCONUS Hire	Identification and Accompanying Armed Forces	2	
	Identification and Identification Privilege	5	
	Two Identification	13	**20**
DoD/ non-DoD Contractor	Identification and Identification Privilege	1	
	Two Identification	28	
	Two Identification Privilege	1	**30**
		Total	**772**

Note: Based on the DMDC data, the 772 contractors had a total of 1,545 CACs: 771contractors each had 2 CACs (771 x 2 = 1,542), and a contractor had 3 CACs, totaling 1,545 CACs (1,542 + 3).

Appendix D. Contract Clauses Governing CAC Recovery

The table below explains the applicability, strengths, and weaknesses of the two standard contract clauses governing the contractor CAC life cycle.

Standard Contract Clause Applicability, Strengths, and Weaknesses

Clause	Applicability	Strengths	Weaknesses
Federal Acquisition Regulation 52.204-9	All DoD contracts; the Contracting Officer inserts after determining that a contractor employee requires "routine" physical or logical access to DoD assets.	1. The clause requires the contractor to comply with agency personal identity verification procedures.	1. "Routine" is open to interpretation, and Contracting Officers may not apply it consistently to contractors. Also, subcontract administrators may not apply it consistently to subcontracts.
		2. The contracting company is required to insert this clause into all subcontracts when its personnel require physical or logical access.	
Air Force Federal Acquisition Regulation Supplement 5342.490-2	All Air Force contracts; inserted after determination that contractor personnel require physical and/or logical access to DoD assets.	1. This clause appears to be required whenever CAC is issued to a contractor.	1. The Air Force Federal Acquisition Regulation Supplement allows the clause or one similar to it to be added to contracts. Therefore, consistency of the strengths and weaknesses in the clause is unknown.
		2. The clause specifies procedures for the contractor to request a CAC.	2. The procedures are outdated and should not include an option to fill out a DD Form 1172-2. Rather, the procedures should require the contractors to use CVS.
		3. This clause addresses CAC return when the contract ends or in certain contingency situations.	3. Contractors have 7 days to return their CAC. It is not clear whether anyone in the Air Force is responsible for ensuring the CAC is recovered when access is no longer required.
		4. The clause instructs contractors to properly display the CAC.	4. The Air Force Federal Acquisition Regulation Supplement does not require contractors to include this clause in subcontracts when subcontractor personnel require physical and/or logical access.
		5. This clause allows the Air Force to withhold final contract payment for violations of the clause.	

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

Final Report Reference

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
TECHNOLOGY
AND LOGISTICS

AUG 29 2008

MEMORANDUM FOR DEPUTY DIRECTOR, JOINT AND OVERSEAS OPERATIONS,
OFFICE OF THE INSPECTOR GENERAL,
DEPARTMENT OF DEFENSE

SUBJECT: Response to DoDIG Draft Report on Audit of Controls Over the Contractor Common Access Card Life Cycle" (Project No. D2007-D000LA-0199.001)

As requested, I am providing responses to the general content and recommendations contained in the subject report.

Recommendation A.1.: We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics direct the Defense Acquisition Regulations Council to include a standard contract clause in the Defense Federal Acquisition Regulation Supplement that, at a minimum, requires contractors to comply with the joint Common Access Card policy in Recommendation A.4. This clause should be applicable to all DoD contracts and subcontracts for which contractor or subcontractor personnel receive Common Access Cards.

Renumbered as Recommendation A.2.

AT&L Response: Concur. AT&L plans to open a Defense Federal Acquisition Regulation Supplement case to address having appropriate regulatory language addressing the requirement for contractors to be accountable for any CACs issued to them, to include return of CACs if the CAC holder no longer needs or is no longer authorized to use the CAC.

Renumbered as Recommendation A.5.

Recommendation A.4.: We recommend that the Under Secretary of Defense for Personnel and Readiness, Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Under Secretary of Defense for Intelligence:

a. Designate within 90 days the lead organization responsible for developing and implementing a joint contractor Common Access Card policy (also see Recommendation D.2.).
b. Implement the joint policy, which at a minimum should require:
    1) Trusted Agents to coordinate with contracting and security personnel when establishing contractors' initial and continued affiliation with DoD and need for Common Access Cards, and to maintain evidence of this coordination;
    2) Standard procedures resulting from Recommendation A.3. for confirming background checks for contractors applying for Common Access Cards;
    3) A limit on the number of contractors a Trusted Agent may sponsor;

Renumbered as Recommendation A.5.

Renumbered as Recommendation A.4.

Final Report Reference

4) Trusted Agents to follow up with contractors who have not returned their Common Access Cards once Recommendation A.2.c. is implemented;
5) Specific Government personnel to recover contractor Common Access Cards when they are no longer needed; and
6) Trusted Agents to inform security personnel when contractors do not return revoked Common Access Cards. In addition, security personnel should consider taking action under section 701, title 18, United States Code.

Renumbered as Recommendation A.3.c.

AT&L Response: Concur. The Under Secretary of Defense for Acquisition, Technology and Logistics will work with the Under Secretary of Defense for Personnel and Readiness and the Under Secretary of Defense for Intelligence to implement these recommendations.

Recommendation D.2.: We recommend that the Under Secretary of Defense for Personnel and Readiness; Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Under Secretary of Defense for Intelligence, incorporate into the joint Common Access Card policy (see Recommendation A.4.), a requirement for Contractor Verification System Service Points of Contact to confirm periodically that Trusted Agent Security Managers and Trusted Agents are authorized to approve contractor Common Access Cards. The joint policy should state how often the Service Points of Contact should perform this action.

Renumbered as Recommendation A.5.

AT&L Response: Concur. The Under Secretary of Defense for Acquisition, Technology and Logistics will work with the Under Secretary of Defense for Personnel and Readiness and the Under Secretary of Defense for Intelligence to implement these recommendations.

Please contact Mr. Craig Howerter at 703-697-8076, Craig.Howerter.CTR@osd.mil if additional information is required.

Philip D. Rodgers
Principal Deputy Director,
Acquisition Resources and Analysis

Under Secretary of Defense for Personnel and Readiness Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-4000

AUG 26 2008

PERSONNEL AND READINESS

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Comments on Draft Report on Controls Over the Common Access Card Life Cycle (Project No. D2007-D000LA-0199.001)

Thank you for the opportunity to review and provide comments on the draft report "Controls Over the Common Access Card Life Cycle," Project No. D2007-D000LA-0199.001, dated July 25, 2008.

We agree with the majority of the findings and recommendations outlined for the Office of the Under Secretary of Defense for Personnel and Readiness. Our comments on the draft report recommendations are included in the Attachment. Please feel free to direct any questions to Mr. Frank Jones (703.696.0179, francis.jones@osd.pentagon.mil) or Ms. Heidi Boyd (703.696.0404, heidi.boyd@osd.pentagon.mil).

Jeanne B. Fites
Deputy Under Secretary of Defense
(Program Integration)

Attachments:
As stated

cc:
Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense for Intelligence
Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer

Final Report Reference

Attachment: Office of the Secretary of Defense For Personnel and Readiness (OUSD(P&R)) Comments to DoD IG Draft Report "Controls Over the Contractor Common Access Card Life Cycle" (Project No. D2007-D000LA-0199.001)

Renumbered as Recommendation A.3.

Recommendations Requiring OUSD(P&R) Comment - Findings A.2:

A.2. "We recommend that the Under Secretary of Defense for Personnel and Readiness:

a. Implement system controls for the Contractor Verification System and the Real-time Automated Personnel Identification System to prevent improper changes to contractor Common Access Card records. System controls should, at a minimum:

(1) Prevent the Real-time Automated Personnel Identification System from:

(a) Issuing Common Access Cards to contractors without the approval of the Trusted Agent in the Contractor Verification System; and

(b) Modifying contractor Common Access Card information approved by the Trusted Agent. When Verifying Officials believe there is an error in the contractor's record, they should direct the contractor to see his or her Trusted Agent so changes may be made.

(2) Ensure all contractor information in the Contractor Verification System (for example, contractor duty country) is accurately transferred to the Defense Enrollment Eligibility and Reporting System/Real-time Automated Personnel Identification System.

Revised

b. Implement procedures to prevent:

(1) Contractors from having multiple active contractor Common Access cards, unless one is for military service, and

(2) Verifying Officials from reissuing contractor Common Access Cards until Trusted Agents have reestablished contractors' DoD affiliation in the Contractor Verification System.

Revised

c. Implement a process that periodically informs Trusted Agents (Government sponsors) when their contractors have not turned in revoked Common Access Cards.

d. Require the Army and Navy Defense Enrollment Eligibility and Reporting System/Real-time Automated Personnel Identification System program offices to rescind the guidance for issuing 3-year Common Access Cards regardless of the contractors' terms of service. Rather, the Army and Navy Defense Enrollment Eligibility Reporting System/Real-time Automated Personnel Identification System

program offices should direct issuance of Common Access Cards in accordance with DoD policy.

e. In accordance with DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007:

(1) Incorporate or convert Under Secretary of Defense Memorandum, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005, into a DoD issuance, reissue the memorandum, or cancel it.

(2) Coordinate with the DoD Chief Information Officer to incorporate or convert Office of the Secretary of Defense Memorandum, "Common Access Card (CAC)," January 16, 2001, into a DoD issuance, reissue the memorandum, or cancel it.

Renumbered as Recommendation A.3.

OUSD(P&R) Response to Recommendations in Findings A.2:

A.2.a.(1)a. OUSD(P&R) concurs with this recommendation. Defense Manpower Data Center (DMDC) will enforce the lock down of the data entry of contractors for Common Access Card (CAC) issuance in October 2008. At that point in time contractor data will only be entered via the Contractor Verification System (CVS).

A.2.a.(1)b. OUSD(P&R) partially concurs with this recommendation. As indicated in the response to A.2.a.(1)a., DMDC will enforce the lock down of the data entry of contractors for CAC issuance in October 2008. At that point in time contractor data will only be entered via CVS. This will also prevent Defense Enrollment Eligibility and Reporting System/Real-time Automated Personnel Identification System (DEERS/RAPIDS) Verifying Officials (VOs) from modifying contractor eligibility data (i.e., CAC expiration date) without approval from the Trusted Agent (TA) via CVS. In order to accurately manage identity in DEERS, certain data fields will remain open for update by the VO in accordance with DEERS/RAPIDS procedures (i.e., name change due to marriage where a scanned marriage certificate is required within DEERS).

A.2.a.(2) OUSD(P&R) concurs with this recommendation. The October 2008 lock down of referenced in A.2.a.(1)a. and A.2.a.(1)b. should help ensure that data input into CVS is accurately transferred to DEERS / RAPIDS.

Revised

A.2.b.(1) OUSD(P&R) concurs in principle with this recommendation as it is already implemented within the Department. Anecdotally, it is possible for an individual to be a DoD civilian, Military Service reservist, adjunct professor, and contractor at the same time with each personnel category qualifying an individual for a separate CAC. However, per DoD policy, only one active CAC can be issued per personnel category, to include that of contractor. All RAPIDS versions currently enforce this policy.

A.2.b.(2) OUSD(P&R) non-concurs with this recommendation. The current process requires CVS TAs to re-verify contractors continued affiliation with DoD and need for CAC card every six months. Any additional re-verification would be redundant and unnecessary. To assist with

Revised

the re-verification process OUSD(P&R) will establish and publish guidelines to assist the TA with the steps necessary to re-verify a record in conjunction with the policy development referenced in the response to A.2.e.(1).

Renumbered as Recommendation A.3.e.(1)

A.2.c. OUSD(P&R) non-concurs with this recommendation. Our office recognizes that there are challenges associated with the retrieval of revoked CACs. However, implementing an automated means to periodically inform TAs when CACs have not been returned will not have the desired effect on tracking revoked cards. DoD has established mechanisms to virtually account for 100% of the CACs that are revoked which would include cards reported lost/stolen, not functioning properly, terminated due to separation, or expired. These cards are shown as inactive within the CAC issuance system and certificates are revoked by the DoD Public Key Infrastructure (PKI). Also, DoD can account for a majority of the cards that have been physically returned to DMDC for disposition. There are, however, an inherent number of cards that cannot be physically accounted for due to the fact that they are lost/stolen, no longer functional, or worn beyond recognition. If CVS TAs were provided periodic reports on CACs that have not been reported as returned, the data could potentially include status information for cards that may have already been returned and destroyed properly. Our office recognizes the need to improve procedures for the return of CACs as a controlled item to include tighter contractual obligations. This will be done via policy and oversight efforts associated with revocation and retrieval as opposed to using automated methods.

Renumbered as Recommendation A.3.c.

A.2.d. OUSD(P&R) concurs with this recommendation. The Defense Human Resources Activity (DHRA) ID Card Policy Office has sent e-mails to the DEERS/RAPIDS Service Project Offices to ensure that contractor CACs are issued with expiration dates in accordance with current policy. It is our understanding that the DEERS/RAPIDS Service Project Offices have rescinded any guidance that is contrary in nature.

Renumbered as Recommendation A.3.d.

A.2.e.(1) OUSD(P&R) concurs with this recommendation. As the designated lead for Homeland Security Presidential Directive-12 (HSPD-12), OUSD(P&R) will incorporate the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) Memorandum, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005, as well as any additional CAC related policies under USD(P&R), into new issuances currently in development. These issuances include the draft Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 and the draft Under Secretary of Defense for Personnel and Readiness DTM 08-003 that outline the Department's roles and responsibilities for CAC-HSPD-12 related items within the scope of this audit. As required by DoD Directive 5025.01, "DoD Directives Program," October 28, 2007, these DTMs will be converted into a DoD instruction within 180 days of their release. Any unaddressed policy related items associated with controls over contractor CACs will be addressed to the maximum extent possible within the DoD instruction.

Renumbered as Recommendation A.3.e.(1)

A.2.e.(2) OUSD(P&R) concurs with this recommendation. See response A.2.e.(1).

Renumbered as Recommendations A.3.e.(2) and A.3.e.(1)

Final Report Reference

Recommendations Requiring OUSD(P&R) Comment - Findings A.4:

A.4. "We recommend that the Under Secretary of Defense for Personnel and Readiness, Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Under Secretary of Defense for Intelligence:

a. Designate within 90 days the lead organization responsible for developing and implementing a joint contractor Common Access Card policy (also see recommendation D.2.).

b. Implement the joint policy, which at a minimum should require:

(1) Trusted Agents to coordinate with contracting and security personnel when establishing contractors' initial and continued affiliation with DoD and need for Common Access Cards, and to maintain evidence of this coordination;

(2) Standard procedures resulting from Recommendation A.3. for confirming background checks for contractors applying for Common Access Cards;

(3) A limit on the number of contractors a Trusted Agent may sponsor;

(4) Trusted Agents to follow up with contractors who have not returned their Common Access Cards once Recommendation A.2.c. is implemented;

(5) Specific Government personnel to recover contractor Common Access Cards when they are no longer needed; and

(6) Trusted Agents to inform security personnel when contractors do not return revoked Common Access Cards. In addition, security personnel should consider taking action under section 701, title 18, United States Code."

Renumbered as Recommendation A.5.

Renumbered as Recommendation A.4.

Renumbered as Recommendation A.3.c.

Renumbered as Recommendation A.5.

OUSD(P&R) Response to Recommendations in Findings A.4:

A.4.a. OUSD(P&R) concurs with this recommendation. As indicated by the response for recommendation A.2.e.(1), OUSD(P&R) is the Department lead for HSPD-12 to include coordination of the policies associated with CAC issuance. Policy development is underway to address the items outlined in recommendation A.4.a.

Renumbered as Recommendation A.3.e.(1)

A.4.b.(1)-(3) OUSD(P&R) concurs with these recommendations. See response A.4.a.

A.4.b.(4) OUSD(P&R) non-concurs with this recommendation. As indicated in the response to A.2.c., OUSD(P&R) recognizes the challenges associated with CAC retrieval. OUSD(P&R) will coordinate and establish CAC retrieval policies and procedures as opposed to attempting to implement the automated notifications referenced in A.2.c.

Renumbered as Recommendation A.3.c.

A.4.b.(5)-(6) OUSD(P&R) concurs with these recommendations. See response A.4.a.

Final Report Reference

Recommendations Requiring OUSD(P&R) Comment - Findings A.5:

A.5. "We recommend that the Director, Defense Manpower Data Center, add a notification screen in the Contractor Verification System which, at a minimum, informs applicants about section 703, title 18, United States Code and explains that revoked Common Access Cards must be returned to specific Government personnel as determined in Recommendation A.4.B.(5)."

Renumbered as Recommendation A.6.

OUSD(P&R) Response to Recommendations in Findings A.5:

A.5. OUSD(P&R) concurs with this recommendation. DMDC will implement a CVS notification message the second quarter of fiscal year 2009 to inform contractor applicants of their responsibility to return terminated or expired CACs to a RAPIDS facility via specific procedures or to specific Government personnel that will be determined during the course of policy development referenced in the response to A.2.e.(1). The notification message will include a reference to *United State Code Section 701 and Title 18*." This information will also be added to the CVS online training and user guide.

Renumbered as Recommendation A.5.B.(5)

Renumbered as Recommendation A.6.

Renumbered as Recommendation A.3.e.(1)

Final Report Reference

Recommendations Requiring OUSD(P&R) Comment - Findings C.1:

C.1. "We recommend that the Under Secretary of Defense for Personnel and Readiness develop and implement the following system controls in the Contractor Verification System and the Real-time Automated Personnel Identification System:

a. Classify contractor pay grade as "Other" and reject incorrect e-mail addresses, as specified in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 3, 2003, for U.S. and foreign national contractors in the Contractor Verification System.

b. Lock the pay grade field for contractors and reject incorrect e-mail addresses, as specified in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 3, 2003, for U.S. and foreign national contractors in the Contractor Verification System.

c. Add a field in the Contractor Verification System for Trusted Agents to record their determination of contractors' need for logical access to DoD networks."

Revised

OUSD(P&R) Response to Recommendations in Findings C.1:

C.1.a. OUSD(P&R) partially concurs with the recommendation to implement system controls to classify pay grades and non-concurs with the recommendation to implement system controls to reject incorrect e-mail addresses.

OUSD(P&R) agrees that inappropriate categorization in the pay grade field is an issue that needs to be addressed for contractors that are eligible for the Geneva Conventions Identification Card for Civilians Accompanying the Forces. Currently RAPIDS, as opposed to CVS, requires capture of a pay grade so that an equivalent Geneva Convention Code Category can be designated in accordance with DoDI 1000.1, "Identity Cards Required by the Geneva Conventions" at the time of CAC issuance. A change to RAPIDS that would designate contractor pay grade as "OTHER" still requires a method to determine the appropriate Geneva Convention Code Category. By the end of calendar year 2008, DMDC will modify RAPIDS to continue to allow RAPIDS VOs to enter pay grades for contractor receiving Geneva Conventions Identification Card for Civilians Accompanying the Armed Forces as currently done to determine the appropriate Geneva Conventions Code Category; however, the printed face of all contractor CACs will only contain "OTHER" for pay grade.

OUSD(P&R) non-concurs with the recommendation to implement CVS and RAPIDS controls to reject incorrect e-mail addresses. E-mail addresses for CAC holders are stored within the DoD PKI e-mail signing and e-mail encryption certificates. These fields have no technical function in CAC-PKI-based website authentication, network authentication, e-mail signing, and e-mail encrypting. The contractor and foreign national designation requirement within DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, is assigned to the network administrators who establish and manage network and e-mail accounts.

Final Report Reference

Enforcing this within the CAC issuance process will not limit any system risk associated with the naming convention of network/email accounts.

C.1.b. OUSD(P&R) partially concurs with this recommendation. See response C.1.a.

C.1.c. OUSD(P&R) non-concurs with this recommendation. During the DoD instruction development process and in coordination with the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), it is expected that more granularity will be added to the definition of CAC eligibility associated with network access. Determination of network logon and the management of these accounts may not necessarily be with the CVS TAs, but with other areas of their organization. It is unclear of the value added in capturing this information within CVS as well as its practicality and enforceability.

Revised

Recommendations Requiring OUSD(P&R) Comment - Findings C.2:

C.2. "We recommend that the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer:

a. Designate within 90 days the lead organization responsible for immediately developing and implementing a recovery plan for contractor Common Access Cards showing improper pay grades and e-mail addresses.

b. Implement the recovery plan for contractor Common Access Cards showing improper pay grades and e-mail addresses"

OUSD(P&R) Response to Recommendations in Findings C.2:

C.2.a. OUSD(P&R) non-concurs with this recommendation. It is recognized that the current CAC infrastructure does not prevent a potentially incorrect or misleading pay grade equivalent from being printed on a contractor's CAC. This will be corrected as referenced in the response to recommendation C.1.a. However, designating a lead and implementing a recovery plan for CACs that are currently in circulation is an action that is out of proportion to the perceived risks cited in the draft report. The Geneva Conventions Identification Card for Civilians Accompanying the Forces CAC for contractors, while potentially indicating an incorrect pay grade, will still indicate that the individual is a "Contractor" or "Foreign Affiliate." There was no specific evidence provided in the draft report that the pay grade area on the card, as opposed to the status or affiliation, was specifically used to authorize any type of access or privileges. Additionally, there are significant cost implications and operational impacts associated with an attempt to recover all CACs with incorrect pay grades and e-mails. The Geneva Conventions Identification Card for Civilians Accompanying the Forces CAC is issued primarily to contractors in Iraq and Afghanistan where the CAC issuance infrastructure is already overburdened at normal capacity. A more appropriate approach given the perceived risk would be to let current CACs be revoked and expire in accordance with the normal life cycles (measured typically in months versus years on deployments) and focus on improving the proper pay grade categorizations for new issuances as described in C.1.a.

C.2.b. OUSD(P&R) non-concurs with this recommendation. See response C.2.a.

Recommendations Requiring OUSD(P&R) Comment -Findings D.1:

D.1. "We recommend that the Director, Defense Manpower Data Center:

a. Develop and implement procedures to:

(1) Verify that Trusted Agent Security Managers and Trusted Agents are Government employees before authorizing sponsorship duties.

(2) Verify that Contractor Verification System sites have active Trusted Agent Security Managers.

b. Establish a plan with defined milestones to identify and deactivate the Contractor Verification System account for all current non-Government Trusted Agent Security Managers and Trusted Agents, and implement this plan."

OUSD(P&R) Response to Recommendations in Findings D.1:

D.1.a.(1) OUSD(P&R) concurs with this recommendation. DMDC will implement procedures through the Security Online System to verify that a Trusted Agent Security Manager (TASM) or TA is a government employee or military member. Until a new release of Security On-line System is available, DMDC is providing reports to CVS Service Points of Contact to review and determine the appropriate corrective action for those identified to be inappropriately designated TASMs and TAs.

D.1.a.(2) OUSD(P&R) concurs with this recommendation. DMDC currently monitors the activity of TASM accounts. If they are inactive for over 45 days, the account is automatically suspended, and after 60 days, the account is deleted. To reactivate an account, the TASM must contact DMDC. This is a passive rather than active approach to ensure sites have active TASMs. Additionally, DMDC notifies the CVS Service Points of Contact when there is a site with an inactive TASM.

D.1.b. OUSD(P&R) concurs with this recommendation. DMDC will periodically provide the CVS Service Points of Contact a list of active TASM and TA to review and determine which individuals should not be TASM or TAs.

Final Report Reference

Recommendations Requiring OUSD(P&R) Comment - Findings D.2:

D.2. "We recommend that the Under Secretary of Defense for Personnel and Readiness; Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Under Secretary of Defense for Intelligence, incorporate into the joint Common Access Card policy (see Recommendation A.4.), a requirement for Contractor Verification System Service Points of Contacts to confirm periodically that Trusted Agent Security Managers and Trusted Agents are authorized to approve contractor Common Access Cards. The joint policy should state how often the Service Points of Contact should perform this action."

Renumbered as Recommendation A.5.

OUSD(P&R) Response to Recommendations in Findings D.2:

D.2. OUSD(P&R) concurs with this recommendation. Procedures and processes will be outlined in the DoD instruction referenced in the response to A.2.e.(1).

Renumbered as Recommendation A.3.e.(1)

Under Secretary of Defense for Intelligence Comments

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

SEP 5 2008

INTELLIGENCE

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Response to the DoD Inspection General (IG) Draft Report, "Controls Over the Contractor Common Access Card Life Cycle," Project No. D2007-D-D000lA-0199.001

In response to the DoD IG's draft report concerning controls over the contractor Common Access Card life cycle supporting Homeland Security Presidential Directive-12 implementation, we submit the attached comments. We appreciate the DoD IG's continued support in achieving full HSPD-12 implementation within the Department.

Where appropriate, we will revise the policies and procedures, and provide security program oversight to enhance the Department's security posture. We participate fully with Federal partners in reforming security and suitability policy, which will address background investigations methods and systems for U.S. persons and foreign nationals. My points of contact are Ms. Andrea Upperman at andrea.upperman@osd.mil or (703) 604-1112, Mr. Stephen Lewis at stephen.lewis@osd.mil or (703) 604-2768, and Ms. Donna Rivera at donna.rivera@osd.mil or (703) 604-1172.

James R. Clapper, Jr.

Attachment:
As stated

Final Report Reference

USD(I) Comments to the Inspector General Draft Report
"Controls Over the Contractor Common Access Card Life Cycle"

USD(I) provides the following general comments:

USD(I) is the Principal Staff Assistant for Industrial, Personnel and Physical Security, in addition to Intelligence and Counterintelligence. Physical Security is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. Under DoD Regulation 5200.08, USD(I) authorizes the use of the Common Access Card (CAC) (in lieu of issuing a security badge) to facilitate physical access to DoD facilities on the premise that the requirements for its issuance and use comply with policy and law. USD(I) will discuss security options with the OSD staff, the U.S. Central Command, and the Military Department staffs to mitigate and resolve vulnerabilities worldwide, as identified.

USD(I) Draft Report Review and Comment

Renumbered as Recommendation A.4.

- **Recommendation A.3:** ***We recommend the Under Secretary of Defense for Intelligence implement policy that, at a minimum, specifies background investigation requirements and the method and system needed to verify the results of the background investigations for both U.S. and foreign national contractors who will be issued Common Access Cards.***

  USD(I) Comment: Federal standards mandate the National Agency Check with written Inquiries (NACI) as the minimum background investigation for HSPD-12 credentialing. Interim credentials may be issued upon a favorable fingerprint check result and the submission of the requisite investigation. We are reviewing solutions to facilitate electronic verification of background investigative results and expect deployment of these solutions by the end of calendar year 2009. USD(I), in partnership with OSD, Service and Agency staff, is working policy guidance that will outline the investigative requirement for CAC credentialing throughout DoD. CAC credentialing standards will apply to all DoD employees, military services, contractors (in staff-like positions, require logical access), or other DoD personnel requiring physical access for 6 months or more.

  Specific guidance to determine credentialing and background investigation standards relating to Foreign Nationals (non-U.S. persons—includes contractors) is under development with the Department of State. CAC issuance to foreign nationals will be limited and strictly controlled.

Final Report Reference

- **Recommendation A.4:** ***We recommend that the Under Secretary of Defense for Personnel and Readiness, Under Secretary of Defense for Acquisition, Technology, and Logistics, and theUnder Secretary of Defense for Intelligence:***
  a. Designate within 90 days the lead organization responsible for developing and implementing a joint contractor Common Access Card policy (also see Recommendation D.2).

  b. Implement the joint policy, which at a minimum should require:
    (1) Trusted Agents to coordinate with contracting and security personnel when establishing contractors' initial and continued affiliation with DoD and need for Common Access Cards, and to maintain evidence of this coordination;
    (2) Standard procedures resulting from Recommendation A.3 for confirming background checks for contractors applying for Common Access Cards;
    (3) A limit on the number of contractors a Trusted Agent may sponsor;
    (4) Trusted Agents to follow up with contractors who have not returned their Common Access Cards once Recommendation A.2.c is implemented;
    (5) Specific Government personnel to recover contractor Common Access Cards when they are no longer needed; and
    (6) Trusted Agents to inform security personnel when contractors do not return revoked Common Access Cards. In addition, security personnel should consider taking action under section 701, title 18, United States Code.

  USD(I) Comment: USD(I) partially concurs with the recommendation in A.4.a. The DoD Common Access Card (CAC) is designated for DoD employees and eligible contractors. USD(I) is the Principal Staff Assistant for Physical Security (access control), Personnel Security (background investigations), and the National Industrial Security Program (contractors). USD(I), in coordination with the Under Secretary of Defense for Personnel and Readiness and the Under Secretary of Defense for Acquisition, Technology, Logistics will develop policy for the DoD CAC, for our areas of responsibility. Contractors who are not eligible for the DoD CAC will receive a local or a DoD alternate physical access only credential (under development by USD(I)). Additionally, USD(I) is developing separate comprehensive security policy for all categories of individuals requiring access to DoD-owned and controlled facilities (worldwide), which will also mandate minimum access control standards, procedures and equipment, including requirements for contractors.

  USD(I) concurs with recommendations as stated in A.4.b. USD(I) will implement appropriate policy as referenced above. Additionally, USD(I) will address

Renumbered as Recommendation A.5.

Renumbered as Recommendation A.4.

Renumbered as Recommendation A.3.c.

Renumbered as Recommendation A.5.a.

Renumbered as Recommendation A.5.b.

Final Report Reference

physical security requirements for CACs, as controlled, U.S. Government property, that require:

(1) the protection of Personal Identity Information;
(2) a reporting requirement for lost/stolen credentials; and
(3) referral to the Department of Justice for violations of Title 18, USC, Section 701 & Title 50, USC, Section 797.

- **Recommendation C.2:** ***We recommend that the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer:***

  a. Designate within 90 days the lead organization responsible for immediately developing and implementing a recovery plan for contractor Common Access Cards showing improper pay grades and e-mail addresses.

  b. Implement the recovery plan for contractor Common Access Cards showing improper pay grades and e-mail addresses.

  USD(I) Comment: USD(I) concurs with the recommendations. Inaccurate information on the CACs poses a security threat and likely may affect accreditation of the system under the Privacy Act of 1974. The Federal credential uses the red color bar to identify First Responders. The color bar on these Common Access Cards issued to contractors (U.S. Citizens and Foreign Nationals) coupled with inaccurate Government civilian pay grades poses a significant vulnerability to Federal facilities worldwide.

- **Recommendation D.2:** ***We recommend that the Under Secretary of Defense for Personnel and Readiness; Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Under Secretary of Defense for Intelligence, incorporate into the joint Common Access Card policy (see Recommendation A.4.), a requirement for Contractor Verification System Service Points of Contact to confirm periodically that Trusted Agent Security Managers and Trusted Agents are authorized to approve contractor Common Access Cards. The joint policy should state how often the Service Points of Contact should perform this action.***

  USD(I) Comment: USD(I) concurs with the recommendation. The OSD staff has convened a working group for the creation of an HSPD-12 implementation and CAC policy and we will address the recommendations stated above.

Renumbered as Recommendation A.5.

Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer Comments

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

AUG 28 2008

MEMORANDUM FOR THE INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Comments on Draft Report "Controls over Contractor Common Access Card Life Cycle" (Project No. D2007-D000LA-0199.001)

Thank you for the opportunity to provide comments to this DODIG report. Our specific comments are provided in the attachment.

The subject report recommends recovery of all Common Access Cards (CACs) with improper pay grades or email addresses. However, immediate recovery and reissuance for a large percentage of CACs falling into this category, e.g., those in use in the Southwest Asia Area of Responsibility (AOR), would be infeasible. Recommend instead that only those CACs that can be tracked to cardholders located in the continental United States (CONUS) be recovered and replaced immediately, and those in the AOR recovered as they expire. This change will not only minimize the mission impact and cost of recovery and replacement, it will also enable the Department to focus on correcting the processes that resulted in improper CAC issuance and recovering improperly issued CACs where the risk to the Department's mission operations is high.

The OASD(NII)/DoD CIO points of contact for this matter are Mr. Morris Hymes, (410) 854-4900, mahyme1@missi.ncsc.mil, and Mr. Don Fuller, (703) 604-5522, ext 112, donald.fuller.ctr@osd.mil.

Robert F. Lentz
Deputy Assistant Secretary of Defense
(Information and Identity Assurance)

Attachment:
As stated

cc:
Under Secretary of Defense for Intelligence
Under Secretary of Defense for Personnel and Readiness
Director, Defense Manpower Data Center

Comments on
DODIG Draft Report "Controls Over the Contractor Common Access Card Life Cycle, Project No. D-2007-D000LA.0199.001"

Recommendations requiring ASD (NII)/DoD CIO comment

Recommendation: *C.2. We recommend that the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense for Intelligence, and the Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer:*

a. *Designate within 90 days the lead organization responsible for immediately developing and implementing a recovery plan for contractor Common Access Cards showing improper pay grades and e-mail addresses.*
b. *Implement the recovery plan for contractor Common Access Cards showing improper pay grades and e-mail addresses.*

ASD (NII)/DoD CIO partially concurs with the recommendation, C.2.

The email address only appears within the signing or encryption certificates of the Contractor Common Access Cards (CAC) and is not displayed on the outside of the card. Use of the card for physical access does not provide access to or expose the email address of the card holder. The number of Contractor CACs used in the Southwest Asia Area of Responsibility (AOR) to authenticate to logical (information) resources where the email address is displayed or exposed is very small and poses little risk to DoD operations. ASD(NII)/DoD CIO intends to work closely with USD(P&R) and USD(I) to develop a recovery plan focused on immediate recovery and reissuance of CACs with improper email addresses only from contractors located in CONUS. Improperly issued CACs currently in use within the AOR will be recovered as they expire. Although recovery and reissuance is important, the immediate focus should be on correcting the issuance procedures resulting in this problem.

U.S. Army Materiel Command Comments

These comments are For Official Use Only. To request a copy, file a Freedom of Information Act request.

Deputy Under Secretary of the Army for Business Transformation Comments

Final Report Reference

DUSA Response to DoDIG Draft Report
Controls Over the Contractor Common Access Card Life Cycle,
Project No. D2007-D000LA-0199.001

B.2. We recommend that the Deputy Under Secretary of the Army for Business Transformation monitor, with DoD personnel, the contractor-run Common Access Card Real-time Automated Personnel Identification System issuance facility collocated with the Kellog, Brown, and Root, Inc. Deployment Processing Center.

Revised

DUSA Response – DUSA disagrees with this recommendation. Our Program Office is not set up to be able to assign personnel to customer sites to monitor their work. We have over 140 task orders and if each one required this level of oversight, we would not be able to operate at our current level of staffing. As a Program Office with contract oversight, we monitor task order performance via In Process Reviews, monthly reports, the quality control plan, dialogue with the contracting officer's representative, etc.

AMC/LOGCAP is the customer who used a DUSA-BT contract vehicle to purchase a requirement that was awarded by the Army's Contracting Center of Excellence. According to the task order, it is the role of the functional representative to conduct quarterly visits. Page 16 of the contract reads as follows – "The LOGCAP Functional Representative serves as the representative who conducts quarterly visits and assesses contractor performance measured against contract performance standards as defined in the PRS." The COR, who is employed by DUSA-BT, is responsible for execution and oversight.

It is true that no COR or other government employee is on-site at the RAPIDS facility. In the past, LOGCAP employees have made site visits to the Houston facility to perform oversight and to ensure security requirements. Additionally, LOGCAP has relied on DCMA employees in the local area to make visits when a government presence is required. Monthly reports from SI Intl indicate that the site was in compliance with contractual requirements.

We recommend that the AMC LOGCAP Office continue to make quarterly site visits to the Houston facility to monitor the CAC distribution process. DUSA will continue to monitor this task order in the same manner that we monitor all of our other 140+ task orders.

Additional comments:

Pages 29-30

Page 22
DoDIG Statement: The DUSA-BT was responsible for monitoring CAC issuance at the SI International RAPIDS site. The DUSA-BT contract was awarded in 3-month option periods.
DUSA Response: The Houston facility is not actually a SI Intl site. It's a KBR site. SII is housed within the site. There have been eight (8) three-month options awarded. However, the current contract was awarded in March 2008 with a base of one year and a

one-year option. Army Oversight of CAC Issuance at the RAPIDS Site Run by SI International

Page 24
DoDIG Statement: DUSA-BT relied on contractors to perform contract oversight. Specifically, SI International, Inc. provided monthly status reports to the contracting officer's representative and functional representative. In these reports, SI International reported its own performance to DUSA-BT, a practice that gave no assurance that contract requirements were being achieved. In addition, the functional representative for the contract was a contractor who was not on-site to assess SI International's performance.
DUSA Response: It is true that SI Intl reports its own performance. However, these monthly (performance) reports are reviewed and accepted by the government functional representative and the quality assurance representative at HRsolutions. Additionally, SI International operates to a Quality Control Plan specific to the task order that is approved by the COR.

The functional representative is actually a government civilian as are all of our 140+ functional reps to the task orders.

Page 32

Page 25
DoDIG Statement: Nine out of thirty CACs were issued without sponsorship based on reviewed DD Forms 1172-2.
DUSA Response: SI Intl does not recall this happening. To their knowledge, all CACs were issued with authorized government signatures. If names can be provided, SI Intl will track.

DoDIG Statement: RAPIDS Verifying Officials modified information approved on DD Form 1172-2 for 2 out of 30 CACs tested.
DUSA Response: This is a partially true statement. SI Intl did change basic data to correct misspellings, etc. However, they did not change pertinent data in reference to entitlements or authorized period of entitlement.

Page 33

Authorizing Official:

25 August 2008

John C. Pastino
Program Manager, HRsolutions Program Office
Office of Deputy Under Secretary Army

U.S. Army Human Resources Command Comments

Final Report Reference

DEPARTMENT OF THE ARMY
U.S. ARMY HUMAN RESOURCES COMMAND
200 STOVALL STREET
ALEXANDRIA VA 22332-0470

AUG 22 2008

AHRC-PDP-P

MEMORANDUM FOR Inspector General, Department of Defense, 400 Army Navy Drive, Arlington, VA 22202-4704

SUBJECT: Department of Defense Inspector General (DODIG) Discussion Draft Report – Controls Over the Contractor Common Access Card Life Cycle (D2007-D000LA-0199.001) (D0808) (FOUO)

1. Thank you for the opportunity to review and comment on the recommendation in your draft report.

Renumbered as Recommendation B.4.

2. I fully concur with DODIG recommendation B.3., that The Adjutant General, U.S. Army Human Resources Command, inform the U.S. Army Defense Enrollment Eligibility and Reporting System/Real-time Automated Personnel Identification System Project Office that it is not permitted to waive DoD policy unless explicitly delegated that authority.

3. Corrective action has been taken to ensure that the Army DEERS/RAPIDS Project Office is in full compliance with DoD ID Card issuance policies and procedures. Specifically, the Project Office has been personally notified that any deviation from DoD policy will not occur without prior coordination and approval from OSD.

REUBEN D. JONES
Brigadier General, USA
The Adjutant General

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Joint and Overseas Operations prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Paul J. Granetto
Donald A. Bloomer
Carol N. Gorman
Melinda M. Oleksa
Dewayne J. McOsker, Jr.
Michael D. Durda
Hanh T. Nguyen
Thomas T. Nguyen
David M. Staley
Anthony M. Torres
Christopher S. Groubert
Dharam Jain
Kandasamy Selvavel
Gregory Collins
Allison E. Tarmann

Inspector General
Department of Defense