Report No. D-2009-086 June 9, 2009

Inspector General
United States Department of Defense

Controls Over the Contractor Common Access Card Life Cycle in the Republic of Korea

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 or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

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

Acronyms and Abbreviations

CAC	Common Access Card
CVS	Contractor Verification System
DEERS	Defense Enrollment Eligibility and Reporting System
DMDC	Defense Manpower Data Center
DoD IG	Department of Defense Inspector General
FKAQ	USFK Assistant Chief of Staff, Acquisition Management
GS	General Schedule
JPAS	Joint Personnel Adjudication System
NACI	National Agency Check with Inquiries
RAPIDS	Real-Time Automated Personnel Identification System
RO	Responsible Officer
SOFA	Status of Forces Agreement
TA	Trusted Agent
TASM	Trusted Agent Security Manager
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USFK	United States Forces Korea

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

June 9, 2009

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
COMMANDER, UNITED STATES FORCES KOREA
DIRECTOR, DEFENSE MANPOWER DATA CENTER

SUBJECT: Controls Over the Contractor Common Access Card Life Cycle in the Republic of Korea (Report No. D-2009-086)

We are providing this report for review and comment. We considered comments on a draft of this report from the Director, Defense Manpower Data Center in preparing the final report. This report is the second in a series on controls over Common Access Cards for contractors.

The Commander, United States Forces Korea did not provide comments on the draft report. DoD Directive 7650.3 requires that all recommendations be resolved promptly. We request the Commander to provide comments on the final report by July 9, 2009.

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 me at (703) 604-8905 (DSN 664-8905).

Paul J. Granetto
Principal Assistant Inspector General
for Auditing

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

What We Did

We determined whether controls over Common Access Cards (CACs) provided to contractors in Korea are in place and working as intended. Specifically, we evaluated whether DoD officials approved and periodically reverified the need for CACs using the Contractor Verification System (CVS) and issued and recovered CACs in accordance with DoD policies and procedures. Information from the Defense Manpower Data Center indicated there were approximately 2,300 contractors with active CACs issued in Korea as of August 31, 2008. This report is the second in a series on CACs issued to contractors.

What We Found

Although supporting documentation for CACs issued to contractors in Korea was generally available, we identified the following internal control weaknesses and areas where additional guidance could improve the administration of contractor CACs:

- 18 of 38 CVS operators interviewed had not taken the required training.
- Expiration dates for CACs were not always consistent with supporting documentation.
- 24 of 37 Trusted Agent sponsors of contractors approved issuance of CACs without verifying the initiation of the required background investigation.
- Guidance for officials who approve and issue CACs was not always clear on what type of identification cards should be issued.
- 56 of the 168 terminated CACs for contractors in our sample could not be accounted for.

Revising existing policy and issuing additional guidance will strengthen controls over contractor CACs in Korea.

What We Recommend

The Commander, United States Forces Korea should improve and issue additional guidance to ensure that an appropriate Responsible Officer is selected, that all contractors requiring a CAC to work in Korea obtain approval from the United States Forces Korea Acquisition Management Office, that CAC expiration dates are consistent with supporting documentation, that personnel approving CACs verify the initiation of background checks, and that terminated CACs are properly recovered.

The Director, Defense Manpower Data Center should establish system controls to prevent CVS operators from sponsoring contractors until the operators have taken the required training, and clarify guidance on the types of identification cards to issue.

Recommendations in DoD Inspector General Report D-2009-005, "Controls Over the Contractor Common Access Card Life Cycle," October 10, 2008, to improve policies and procedures are being implemented and are not repeated in this report.

Management Comments and Our Response

The Commander, United States Forces Korea did not provide comments on the draft report, dated March 13, 2009. We request the Commander to provide comments on the final report by July 9, 2009. The Director, Defense Manpower Data Center provided responsive comments to the recommendations and is implementing corrective actions. The Director also provided comments on the finding. See the recommendations table on page ii.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Commander, United States Forces Korea	1.	
Director, Defense Manpower Data Center		2.

Please provide comments by July 9, 2009

Table of Contents

Introduction

Objectives

The overall objective of this audit was to determine whether controls over Common Access Cards (CACs) provided to contractors in the Republic of Korea (Korea) were in place and working as intended. Specifically, we determined whether DoD officials issued CACs to contractors according to the requirements of the Contractor Verification System (CVS), verified the continued need for contractors to possess CACs, and revoked and recovered CACs from contractors in accordance with DoD policies and procedures. See the Appendix for a discussion of the scope and methodology and prior coverage related to the objectives.

Background

In October 2000 DoD began issuing CACs to active-duty 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.

Contractor CAC Life Cycle

The contractor CAC life cycle consists of four phases: application and approval, issuance, reverification, and revocation and recovery. The application and approval phase begins when a contractor requests a CAC through CVS. After the sponsor, the Trusted Agent (TA), approves the application in CVS, the contractor reports to a Real-Time Automated Personnel Identification System (RAPIDS) site to be issued a CAC. After issuance, a TA must verify every 180 days that the contractor still needs a CAC. When the contractor no longer needs or is authorized a CAC, the CAC is revoked and recovered. Finally, RAPIDS personnel send the recovered CACs they receive from TAs or RAPIDS sites to the Defense Manpower Data Center (DMDC) for destruction.

Systems Used To Process Contractor CACs

A memorandum from the Under Secretary of Defense for Personnel and Readiness (USD[P&R]) titled, "DEERS/RAPIDS Lock Down for Contractors," November 10, 2005 (hereafter the USD[P&R] Memorandum), mandated the use of CVS to apply for and authorize a contractor CAC commencing in July 2006. 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. However, DMDC did not enforce this mandate until the end of October 2008, when a program change to the RAPIDS software prevented operators from issuing CACs to contractors who could not be verified through

CVS. RAPIDS is a system that retrieves contractor records from DEERS and prints the information on CACs for issuance.

The DMDC Contractor Verification System User Manual (hereafter the CVS User Manual), Version 2.0, December 2008,[1] requires a TA, a U.S. citizen and Government employee sponsoring a contractor, to use CVS to approve the application of a contractor needing to obtain a CAC. The TA 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 Identity Verification (PIV) of Federal Employees and Contractors," March 2006.
- Establish the contractor's need for logical and physical access and the duration of access to DoD networks or facilities.
- Verify that contractors have had required background checks initiated.

Previous Audit Findings and Recommendations

Department of Defense Inspector General (DoD IG) Report D-2009-005, "Controls Over the Contractor Common Access Card Life Cycle," October 10, 2008, the first report in this series, found that 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 the appropriate background checks.
- RAPIDS personnel changed information approved by Government sponsors.
- DoD did not always recover revoked contractor CACs.
- The Army did not provide adequate oversight of thousands of CACs issued to contractors deploying to Southwest Asia.

Overall, the CAC life-cycle weaknesses found posed a potential national security risk that could allow unauthorized access to DoD resources, installations, and sensitive information. To tighten controls over contractor CACs, the report recommended implementing improved DoD policies, procedures, and oversight as well as additional system controls over CVS and RAPIDS.

The Office of the Secretary of Defense and the Army generally agreed with our recommendations and began making improvements in policies and controls. In this report we do not duplicate recommendations made in the prior report. However, we will continue to monitor actions proposed by DoD to ensure their implementation.

---

[1] The DMDC CVS User Training Guide, Version 1.9.2, August 2007, which was in force during the audit period, had similar guidance.

Review of Internal Controls

We identified internal control weaknesses in the administration of contractor CACs related to the training of CVS operators, verification of contractor background checks, and accountability for terminated CACs. Actions taken or planned by DoD in response to DoD IG Report D-2009-005 should correct most of the problems except that DMDC needs to establish a date by when it will prohibit personnel from becoming CVS operators if they have not taken the required training. To further strengthen controls over verification of contractors' backgrounds and accountability for terminated CACs, USFK should implement Recommendation 1., parts d. and e. We will provide a copy of the final report to the senior official for internal controls at USFK.

Finding. Common Access Cards Issued to Contractors in Korea

Although supporting documentation for CACs issued to contractors working in Korea was generally available, we identified the following internal control weaknesses and areas where additional guidance could improve the administration of contractor CACs.

- At least 18 of 38 CVS operators interviewed had not taken the required training.
- Expiration dates for CACs issued in Korea did not always agree with supporting documentation.
- 24 of 37 TA sponsors of contractors approved issuance of CACs without verifying the initiation of the required background investigation.
- Nine contractors in our sample received the wrong type of identification card.
- Of 168 terminated CACs associated with our sample of contractors in Korea, 56 were not properly accounted for.

The weaknesses identified increase the risk of unauthorized access to DoD resources, installations, and sensitive information. Establishing and implementing the DoD-wide policy, procedures, and controls recommended in the prior DoD IG report on the contractor CAC life cycle; clarifying DMDC guidance regarding the correct types of identification cards to issue; and issuing additional policy guidance and controls for USFK will strengthen controls over contractor CACs in Korea.

Analysis of CAC Data

To review controls over CAC applications and CACs issued in Korea, we requested data from DMDC on CAC applications entered in CVS and on CACs issued from RAPIDS sites in Korea for the year ended August 31, 2008. We combined these two data sets to establish a universe of contractors to review. After we selected a random sample of contractors, we determined that DMDC had incorrectly included dependents of contractors (who were not issued CACs) and contractors not associated with Korea in the populations provided. Therefore, we are unable to project from our sample to the total population. However, we believe that the results of our review are representative of procedures and conditions related to CACs applied for and issued to contractors in Korea. We selected a random sample of 177 contractors from a data population of 2,601 contractor records representing contractors who had applied for or obtained CACs in Korea during the audit period.[2] See the Appendix for additional details regarding the data populations and sample selection.

Training for CVS Operators

The CVS User Manual requires CVS operators, known as Trusted Agent Security Managers (TASMs) and TAs, to complete annual certification training courses in order to

[2] Some contractors were issued more than one CAC during the period because a previous CAC was terminated.

access CVS and perform their duties. However, CVS was not set up to prevent TASMs and TAs from logging on to CVS before completing the required training. Interviews with 38 TASMs and TAs in Korea associated with the contractors in our sample indicated 18 (47 percent) had not taken the required certification training. The lack of training sometimes caused problems for TASMs and TAs in performing their required functions, as the following examples illustrate.

- A TASM did not know how to transfer contractors to a new TA when the previous TA moved to another position. Therefore, instead of reassigning contractors, the TASM created new applications under his account.
- A TA did not use CVS to sponsor contractors who possessed CACs from prior years, and did not reverify these CACs as required.
- A TA cut up recovered CACs and disposed of them instead of turning them in to a RAPIDS site, as required.
- A TA gave his CVS username and password to his predecessor to use in completing a contractor application because the new TA had not taken the required training and was unfamiliar with CVS.

DMDC personnel stated that, beginning in January 2009, CVS operators started receiving warnings when logging on to the system if they had not completed the required training. However, to further strengthen this control, DMDC should modify CVS to prohibit TAs and TASMS from logging on to CVS if they have not completed the required certification training. DMDC personnel stated that they planned to implement this control.

CAC Application and Approval

In accordance with the Federal Information Processing Standards Publication 201-1 and the CVS User Manual, the TA must establish the contractor's affiliation with the Government and the person's need for logical and physical access. We were able to obtain sufficient documentation to support DoD affiliation for 170 of 177 contractors in our sample. However, for the remaining seven contractors, we could not verify affiliation with DoD for the following reasons.

- A TA completed a CVS application for a contractor based on an e-mail from another contractor rather than verifying the contractor's affiliation with the Government.
- The TAs for two contractors could not provide any evidence of why the contractors received CACs in Korea. The CACs for both contractors had been terminated before our audit began.
- Three contractors were not in CVS, and no documentation was available to support their CACs.
- The TA for one contractor, a Korean national, could not provide adequate support for issuing her a CAC.

As for the 170 contractors whose affiliation with DoD we were able to confirm, sufficient documentation was often available because many TAs were also the Responsible Officers

(ROs) for their contracts. The TAs for 91 contractors also functioned as ROs (or direct subordinates), overseeing contactors closely. These TAs had ready access to information they needed to determine contractors' affiliation with DoD and need for CACs. According to USFK Regulation 700-19, "The Invited Contractor and Technical Representative Program,"[3] June 4, 2007, ROs should be geographically and functionally situated to enable direct personal contact with the contractor being sponsored, certify the contractor's entitlements to logistics support, and maintain the supporting documentation. If USFK had a policy requiring ROs or their direct subordinates to be TAs for contractors working in Korea, when practical, USFK could strengthen controls over approval and monitoring of contractor CACs.

USFK Regulation 700-19 requires approval from the Office of the Assistant Chief of Staff for Acquisition Management (FKAQ) and the Status of Forces Agreement (SOFA)[4] Joint Committee before invited contractors to Korea are granted SOFA status. SOFA status normally entitles invited contractors who are "ordinarily" residents of the United States to logistical support privileges. This regulation further requires the sponsoring agency or RO to submit for FKAQ approval a copy of the contract information, a letter of accreditation, and an Invited Contractor and Technical Representative Personnel Data Report (USFK Form 700-19A-R-E). Upon approval, the contractor takes the required forms to the RAPIDS site to obtain an Identification and Privilege CAC. A CAC with privileges entitles the contractor to logistical support, which normally includes access to the post or base exchange; Morale, Welfare, and Recreation facilities; and the commissary.

USFK Regulation 700-19 requires contractors needing an identification card, logistical support, and SOFA status to prepare and submit to FKAQ a USFK Form 700-19A-R-E that has been approved by the contractor's RO. FKAQ maintains this documentation, which enabled us to verify the Government affiliation of many contractors if the TA did not have the documents or was unavailable for interview. However, not all contractors needing a CAC go through FKAQ. Contractors hired from the pool of retired military personnel and dependents of invited contractors, military, or civilian personnel assigned to Korea sometimes do not go through FKAQ because they already have an identification card to access facilities on the military installation. Also, U.S. citizens and third-country nationals who are residents of Korea working on a contract supporting USFK are not necessarily eligible to receive an Identification and Privilege CAC and might not obtain approval from FKAQ. An FKAQ official stated that this limitation has also hindered assessment of the contractor population for a potential noncombatant evacuation operation.

---

[3] For audit purposes, we did not differentiate between an invited contractor and a technical representative. Some technical representatives were contractors. Others were representatives for commercial companies. If these individuals needed CACs, they would use CVS.

[4] The SOFA is an international agreement between the United States and Korea envisaged by Article IV of the United States Republic of Korea Mutual Defense Treaty. The SOFA discusses facilities, areas, and the status of the U.S. Armed Forces in Korea.

FKAQ personnel stated that USFK may revise the regulation to extend its applicability to every contractor performing services for USFK in Korea. We support this planned revision to require FKAQ approval for all contractors working in Korea to obtain a CAC. Once revised, the regulation will also help document validation of contractor CACs.

CAC Expiration

A memorandum signed by USD(P&R) and the DoD Chief Information Officer titled "Common Access Card (CAC)-Changes," April 18, 2002, allows CACs to be issued for 3 years or the individual's term of service, employment, or association with DoD, whichever is shorter. USD(P&R) Directive-Type Memorandum 08-003, "Next Generation Common Access Card Implementation Guidance," December 1, 2008, updated the 2002 guidance. The new memorandum allows a CAC to be issued for the duration of the contract, including unfunded options up to 3 years. (In Korea a CAC is normally issued for the funded portion of the contract, usually 1 year or less.)

However, neither TAs nor RAPIDS operators used consistent criteria for entering the CAC expiration date in CVS or RAPIDS. Although the expiration of most CACs was based on the funded portion of the contract as shown on USFK Form 700-19A-R-E, CACs for 62 contractors in our sample expired 30 days after the contract expiration date shown on the form. Such inconsistencies occurred because CVS and RAPIDS operators did not have clear guidance for CAC operations in Korea. Operators allowed the extra 30 days in accordance with USFK Regulation 700-19, which states that a contractor's status shall automatically be withdrawn 30 days after termination of a contract. The extra days were given for a contractor to renew the CAC based on new contract funding or leave Korea.

It is reasonable to allow a contractor some time to renew a CAC after the funded portion of a multiyear contract expires. However, there is no basis for extending the expiration of a CAC by 30 days for a completed contract. Therefore, USFK should clarify guidance to all TAs in Korea emphasizing that the expiration date for a contractor CAC should not be later than the completion of a contract.[5] USFK may also wish to issue CACs for up to 3 years for contractors on multiyear contracts as allowed by Directive-Type Memorandum 08-003.

Contractor Background Investigations

Of the 37 TAs interviewed during the audit, 24 did not verify the status of contractors' background checks. Some of the reasons TAs gave for not verifying that a background investigation had been initiated were the following.

- They believed some other USFK organization or the contractor had this responsibility.
- The contractor did not work on classified material.

[5] Guidance is not needed for RAPIDS operators because system changes completed in November 2008 prevent RAPIDS operators from changing the expiration shown in CVS when issuing a CAC.

- They did not know what they were supposed to do.
- They were unaware that a National Agency Check with Inquiries (NACI), or the equivalent, must be initiated before the issuance of a CAC.

We used the Joint Personnel Adjudication System (JPAS), which provides real-time information regarding security clearances, access, and investigative status, to check the status of background investigations for contractors. According to information in JPAS, no NACI had been initiated for 50 of the 177 contractors in our sample. After we issued the draft report, we learned that JPAS may not contain information on background investigations for some contractors who do not require access to classified information. Therefore, the number of contractors with CACs who did not have a NACI initiated is not certain. However, our interviews with TAs responsible for verifying that background investigation requirements have been met indicate that contractors can obtain CACs without going through the required investigations.

The CVS User Manual provides no guidance to the TA on how to determine whether a proper background check has been initiated. In addition, CVS does not require TAs to indicate contractor's background status when completing the CVS application. In fact, the system contains no field to indicate the status of a background check.

Federal Information Processing Standard 201-1 requires contractors seeking a CAC to have an initiated NACI or an equivalent background investigation. At a minimum, the Federal Bureau of Investigation National Criminal History Check (fingerprint check) must be completed before a CAC can be issued. 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.

DoD IG Report D-2009-005 raised a similar issue regarding the need for specific background investigation requirements and standard procedures for confirming background checks for contractors applying for CACs. The Under Secretary of Defense for Intelligence noted in response to that report that an electronic system will be deployed by the end of 2009 to facilitate electronic verification of background checks. The Under Secretary also stated that his office is working on policy guidance that will outline the investigative requirements for CAC credentialing throughout DoD. DMDC personnel stated during our audit that the latest version of RAPIDS interfaces with JPAS but does not prevent a CAC from being issued when there is no indication of a NACI in JPAS.

USD(P&R) Directive-Type Memorandum 08-003, which was issued during our audit, gives further guidance on conducting background investigations of contractors, including an authoritative list of background investigations that are equivalent to or exceed the requirements of a NACI, and actions that should be taken by Government sponsors of contractors requiring a CAC. However, until DMDC implements a system change prohibiting CACs from being issued to contractors for whom a NACI has not been initiated, USFK should provide guidance for TAs, outlining standard procedures to confirm that a NACI (or equivalent investigation) has been initiated, as required by Federal and DoD regulations. Such procedures could require TAs to obtain contractor

verification that a NACI has been initiated, or to verify the contractor's status at the local personnel security office.

CAC Issuance

Before issuing a CAC to a contractor, RAPIDS operators should ensure at a minimum that a contractor profile was established in DEERS through CVS and that the CAC, as issued, correctly reflects the duration of the contractor's work and the benefits the contractor is entitled to.

Data Source for DEERS Profile

The USD(P&R) Memorandum designated CVS as an authorized source of contractor's data to be fed into DEERS as of July 31, 2006. However, at the time of our review, not all contractor CACs had been entered in CVS. For example, a TA stated that she did not use CVS to manage contractors needing to receive new CACs if the contractors received their original CACs before CVS implementation. According to the CVS User Manual, a TA should use CVS to sponsor applicants who have previously had CACs. In another instance, a TA did not use CVS to authorize a CAC because he thought that use of CVS was not required for a Korean subcontractor of a contractor authorized and invited by USFK.

In both instances, RAPIDS operators issued CACs to contractors who were not entered in CVS because the lock down mandated by the USD(P&R) Memorandum had not taken place. According to DMDC, during November 2008, a system control was added to RAPIDS that prevents RAPIDS operators from issuing a CAC to any contractor without CVS verification. Therefore, we are not making any recommendation regarding the use of CVS for approving CACs.

Types of Identification Cards

Of 177 contractors in our sample, 9 received inappropriate identification cards because guidance for TAs and RAPIDS operators was not clear about the type of identification card to issue.

Identification and Privilege CACs

Identification and Privilege CACs were issued to two entertainers and four summer-hire student contractors who came to Korea to work under contracts supporting Morale, Welfare, and Recreation for less than 3 months. (The audit universe from DMDC also included 30 student contractors who received CACs but needed only physical access to DoD facilities for less than 3 months.) The entertainers and students were ineligible for a CAC based on:

- Air Force Instruction 36-3026(I), "Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible

Personnel,"[6] December 20, 2002, and USD(P&R) Directive-Type Memorandum 08-003, which state that an Identification and Privilege CAC is issued to contractors who are stationed or employed overseas for 365 days or more; and

- USD(P&R) Directive-Type Memorandum 08-003, which further states that contractors are eligible for a CAC when they require physical access to multiple Government facilities on a recurring basis for at least 6 months or require both physical and logical access to DoD installations and networks.

According to the sponsoring TAs, these contractors did not need and were not given access to DoD networks. Without a need for physical access for 6 months or the need for both physical and logical access, these individuals should not have received CACs. Rather they should have been issued a base pass and an appropriate ration card to obtain access to USFK facilities. This was also the case of a contractor who was issued an Identification CAC for 13 days. None of those seven contractors were eligible for any type of CAC.

To ensure that only eligible contractors receive CACs and that they receive the correct type of CAC, TAs and RAPIDS operators must be able to determine who is eligible for a CAC and for what type of a CAC. However, the CVS User Manual does not list specific criteria for CAC eligibility; it states only that TAs must establish a contractor's need for physical and logical access. Also, the RAPIDS User Guide issued by DMDC, while stating that contractors are eligible for an Identification and Privilege CAC when going on assignment overseas, is not clear about the duration of overseas assignments required for a contractor to obtain an Identification and Privilege CAC. Because TAs and RAPIDS operators use the CVS User Manual and RAPIDS User Guide as references for their CAC operations, those documents should state the eligibility requirements for each type of CAC to ensure compliance with DoD guidance.

Geneva Conventions CACs

Geneva Conventions CACs should be issued to "emergency essential" contractors accompanying and supporting the Armed Forces during a conflict, combat, or contingency operation. However, RAPIDS operators issued Geneva Conventions CACs to two contractors in our sample who were not identified as emergency essential, partly because the RAPIDS User Guide was not clear about the eligibility for a Geneva Conventions CAC. The RAPIDS User Guide states that contractors accompanying forces overseas for more than 1 year are entitled to a Geneva Conventions CAC, but does not state what constitutes contingency conditions. To ensure that only eligible contractors receive the benefits under the Geneva Conventions agreement, the RAPIDS User Guide needs to provide clear guidance for RAPIDS operators to determine who is eligible for a Geneva Conventions CAC.

---

[6] Air Force Instruction 36-3026(I) is a joint service regulation, also referred to as Army Regulation 600-8-14, Bureau of Naval Personnel Instruction 1750.10B, Marine Corps Order P5512.11C, and Commandant Instruction M5512.1.

Misclassification of Contractors

Of the 2,601 contractors in our audit universe, 146 contractors (5.6 percent) were inappropriately assigned a General Schedule (GS) pay grade because RAPIDS did not include controls to limit pay grade entries as GS-Equivalent or Other for contractors. Misclassification of contractors can affect their entitlements and access to information. Contractors may receive housing available only to U.S. Government personnel and gain access to sensitive information that may be restricted to Government employees. Misclassification of pay grade could be prevented by system controls that limit entry options to the pay grade class designated for contractors. In response to DoD IG Report No. D-2009-005, regarding CACs erroneously showing GS pay grades, the USD(P&R) stated that DMDC will modify RAPIDS so that the printed face of all contractor CACs will show Other for the pay grade. Therefore, we are not making any recommendation to correct misclassification.

CAC Reverification

The CVS User Manual states that the TA should reverify a contractor's need for a CAC every 180 days. When a contractor reaches the 150-day mark, the TA receives e-mail notification from CVS to reverify the contractor's need for the CAC. The TA has 30 days after this notification to reverify, or the contractor's CAC will automatically be revoked.

USFK has a policy whereby invited contractors working in Korea are issued a CAC only for the funded portion of a contract, normally not more than 1 year. This control reduced the risk of unauthorized use of CACs, compared with the multiyear contracts or the maximum 3-year period allowed by DoD.

The majority of TAs interviewed stated that they took steps to reverify each contractor's employment status; however, they did not normally maintain documentation to support their reverification. Therefore, an audit trail was not available for us to confirm that TAs had assessed each contractor's continued need for a CAC at the time of reverification. However, as previously discussed, having a TA who is also the RO facilitates verification of a contractor's status. Requiring TAs to be ROs would further reduce the risk of contractors having unauthorized CACs after their association with the Government has terminated.

CAC Revocation and Recovery

The CVS User Manual states that the TA should collect and return revoked and expired CACs in accordance with standard procedures. Upon receipt of such CACs, the RAPIDS Site Security Managers return the CACs to DMDC. When DMDC receives the terminated CACs, DMDC updates their status in the Inventory Logistics Portal, the system for inventory and logistic management of CAC card stock. This action indicates that the CACs have been revoked, recovered, and prepared for destruction.
In Korea, ROs are responsible for recovering CACs when contractors finish their work or leave Korea. USFK Regulation 700-19 requires ROs to collect and return identification cards to the issuing authorities. ROs must document turn-in of the identification cards on

USFK Form 700-19A-R-E, Part IV, and submit the closeout form to FKAQ. However, in discussions with us, FKAQ personnel indicated that they do not receive copies of the completed USFK Form 700-19A-R-E for contractors finishing their work or leaving Korea.

Of the CACs issued to contractors in our sample, 168 were terminated.[7] DMDC verified that 112 of these CACs had been recovered and returned to DMDC. Of 56 CACs not returned, only 4 were coded as lost. In responding to the draft report, DMDC stated that it cannot account for all CACs returned, because some CACs returned to DMDC are no longer functional and are worn beyond recognition. However, in our opinion the main inability to account for all CACs occurred because TAs and ROs did not comply with the CVS User Manual or USFK Regulation 700-19. Some TAs or ROs we interviewed did not even know that they were responsible for recovery of CACs. One TA stated that he cut up expired CACs but did not document which CACs he destroyed. Enforcing the requirement for TAs to take the annual certification training should make operators aware of their responsibilities and provide full accountability.

In response to DoD IG Report No. D-2009-005, DMDC agreed to include a message for contractors applying for a CAC in CVS, informing the applicants of their responsibility to return terminated or expired CACs to a RAPIDS facility or to specific Government personnel (such as a TA). In addition, USD(P&R) agreed to implement a process to periodically inform TAs when contractors have not turned in revoked CACs. USD(P&R) was working on guidance requiring local commands to ensure that retrieval of CACs is part of the normal check-out process. When fully implemented, these actions will further strengthen controls over recovery of CACs.

USFK should enforce and monitor compliance with USFK Regulation 700-19 to ensure CACs are properly recovered when contractors do not need them for official business with the Government.

Compensating Controls Over Physical Access

To gain access to military installations in Korea, CAC holders must register their CACs with the Defense Biometric Identification System. Security personnel at the access control point use the Defense Biometric Identification System to verify the authenticity of all CACs. When a CAC is suspicious or questionable, the access control point security personnel verify its authenticity by using the fingerprint scan function of the system. Therefore, the Defense Biometric Identification System precludes possible use of invalid, lost, or stolen CACs for installation access. Also, to be granted access to the post or base exchanges and commissaries, CAC holders must present a valid CAC and a Ration Control Card at the same time. To obtain the Ration Control Card, contractors must register in the Defense Biometric Identification System. These internal controls

[7] Some contractors had more than one CAC terminated for various reasons, such as changes in information or issuance failure. Other contractors did not have a CAC that was terminated during the audit period.

compensate for control weaknesses and reduce the risk of unauthorized access to DoD installations and privileges in Korea.

Conclusion

Although supporting documentation for CACs issued to contractors in Korea was usually available, strengthening controls and issuing additional guidance could improve the administration of contractor CACs. Compensating controls, such as the use of the Defense Biometric Identification System and review of contracts by FKAQ, helped reduce the security risk. After we issued DoD IG Report D-2009-005, DoD issued guidance and made system changes to improve the administration of contractor CACs. DoD has stated that additional policy and system improvements will be forthcoming. These improvements should resolve most of the weaknesses identified in this report. However, implementing the recommendations in this report should resolve the remaining weaknesses and further reduce potential national security risks posed by unauthorized access to DoD resources, installations, and sensitive information.

Management Comments on the Finding and Our Response

DMDC Comments

The Director, DMDC did not believe that we had sufficient support for our characterization of the weaknesses in controls in the previous CAC audit (D-2009-005) as a "potential national security risk." A specific example in the previous report regarding the potential risk gave the impression that an e-mail address contained in a CAC could allow a contractor access to assets. A CAC is only an identification card that alone should not provide its holder access to DoD networks or facilities. The requirement shown in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, to identify contractors by their e-mail addresses is assigned to network administrators, who establish e-mail accounts and manage network access.

The Director stated that JPAS does not contain suitability determination information for individuals who do not require access to classified information. Therefore, the DoD IG's use of JPAS alone to verify background investigations for contractors failed to account for all of the systems that contain suitability information for contractors.

The Director stated that the audit report implied that DMDC was able to account for all CACs that were physically returned to DMDC. However, sometimes returned CACs cannot be identified because they are no longer functional or are worn beyond recognition.

Our Response

The DMDC disagreement with our use of the phrase "potential national security risk" was related to a previously issued audit report. Report D-2009-005 identified numerous deficiencies and gave several examples to back up the audit conclusions. The conclusion of the report was that "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." We consider the example cited in the DMDC comments regarding contractor e-mail accounts as one of many potential weaknesses identified in the previous audit report. For example, if a contractor with a DoD (.mil) e-mail account is not identified as a contractor, U.S. Government personnel may send the contractor information that is only authorized for U.S. Government employees and *could* be a potential national security risk.

We used JPAS as one source of information on the status of required investigations for contractors. Information provided to us by DMDC after we issued the draft report indicates that JPAS may not have all information on the suitability determinations for contractors. Therefore, we modified our report accordingly. However, Recommendation 1.d. remains the same because it is the TA's responsibility to verify that a NACI has been initiated.

We did not mean to imply that DMDC could account for all CACs that were returned. Our audit focus was on whether TAs were properly accounting for or returning CACs that were expired or invalid. We merely stated how many of the terminated CACs DMDC could account for. We clarified our report to indicate that some returned CACs cannot be identified because they cannot be read.

Recommendations, Management Comments, and Our Response

1. **We recommend that the Commander, United States Forces Korea:**

a. Require a Responsible Officer or a direct subordinate to be the Trusted Agent for contractors sponsored in Korea, when practical.

b. Revise United States Forces Korea Regulation 700-19 to require all contractors working in Korea who require a Common Access Card to obtain approval from the Office of the Assistant Chief of Staff, Acquisition Management.

c. Issue guidance to Trusted Agents approving contractor Common Access Cards in Korea emphasizing that the expiration date for the card must not be later than the date of contract completion.

d. Require Trusted Agents to verify that a National Agency Check with Inquiries has been initiated before they approve a contractor's application for a Common Access Card in the Contractor Verification System.

e. Enforce and monitor compliance with United States Forces Korea Regulation 700-19 to ensure contractor Common Access Cards are properly recovered and turned in to the appropriate Real-Time Automated Personnel Identification System site when the cards expire or are no longer needed for official business with the Government.

Management Comments Required

The Commander, USFK did not respond to the draft report. We request the Commander to provide comments on the final report by July 9, 2009.

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

a. Modify the Contractor Verification System to prohibit Trusted Agent Security Managers and Trusted Agents from using the system if they have not taken the required certification training.

Defense Manpower Data Center Comments

The Director, DMDC agreed and stated that by August 2009 DMDC will require operators to complete certification training. After a 30-day warning period, TAs and TASMs who have not completed the required training will be locked out of their CVS accounts.

b. Clarify the Real-Time Automated Personnel Identification System User Guide by listing eligibility requirements that contractors must meet for the Identification and Privilege Common Access Card and the Geneva Conventions Common Access Card.

Defense Manpower Data Center Comments

The Director, DMDC agreed and stated that as of March 19, 2009, the RAPIDS 7.4 User Guide includes updates to clarify both eligibility and documentation requirements for contractors.

c. Clarify the Contractor Verification System User Guide to help a Trusted Agent determine whether or not a Common Access Card or a base pass should be issued to a contractor who needs physical access to Government facilities for short periods.

Defense Manpower Data Center Comments

The Director, DMDC agreed and stated that DMDC, in coordination with the Defense Human Resource Activity, will update the CVS User Guide to improve the explanation of CAC eligibility by August 2009.

Our Response

DMDC comments on all parts of Recommendation 2. were responsive, and no additional comments are required.

Appendix. Scope and Methodology

We conducted this performance audit from September 2008 through February 2009 in accordance with generally accepted government auditing standards. 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 interviewed the Site Security Managers and Verifying Officials regarding their procedures and operations at the 10 RAPIDS sites in Korea: U.S. Army Yongsan Garrison, Camp Red Cloud, Camp Stanley, Camp Casey, Camp Humphreys, Camp Henry, Osan Air Base, Kunsan Air Base, Chinhae Naval Base, and the Navy Personnel Support Detachment at Yongsan.

At our request, DMDC provided four data sets that corresponded to each phase of the contractor CAC life cycle:

- CVS applications associated with Korean CVS site operators or CACs issued or terminated by a Korean RAPIDS Site from September 1, 2007, through August 31, 2008 (application data);
- CACs issued from the Korean RAPIDS site from September 4, 2007, through September 12, 2008 (issuance data);[*]
- CVS reverifications associated with Korean CVS site operators or CACs issued or terminated by a Korean RAPIDS site from September 1, 2007, through August 31, 2008; and
- CACs terminated from the Korean RAPIDS site from September 1, 2007, through September 12, 2008.[*]

After a preliminary review of those data sets, we decided to use the application data and issuance data to obtain a universe of contractors. After merging two data sets and eliminating duplicates, we sent data on the universe of 3,568 contractors to the DoD IG Quantitative Methods and Analysis Division for selecting a statistical random sample of 252 contractors. As the audit progressed, we found that the CAC issuance data provided by DMDC incorrectly included contractor dependents, who received dependent identification cards rather than CACs. Therefore, we had to delete 967 records from the audit universe, reducing the population to 2,601. (Note that the audit universe is greater than the number of contractors issued CACs in Korea as of August 31, 2008 [approximately 2,300], because the audit universe included contractors who were issued CACs that may have terminated before August 31, 2008.) As we examined the supporting documentation for CACs issued, we also found that DMDC had incorrectly

[*] We asked DMDC for CVS and RAPIDS information for the year ended August 31, 2008. However, DMDC used slightly different dates, as shown above. The use of different dates did not affect our audit conclusions

included some contractors who were not issued CACs in Korea. This reportedly happened because DMDC incorrectly selected contractors associated with a TA who had at one time been associated with Korean contractors. As a result, we reduced the sample to 177 contractors. Therefore, we were not able to project from our sample to the universe. Consequently, we analyzed the results for our random sample and presented our findings based on this analysis. However, because the contractors were selected at random, we reasonably believe that the results are representative of the universe.

For each contractor in our sample, we tested specific steps in the CAC life cycle. For contractors whose applications DMDC data indicated were processed through CVS, we also interviewed the TAs, if available. We interviewed 38 TASMs and TAs (many TASMs also functioned as TAs) responsible for sponsoring contractors in Korea to determine their functions, what training they had taken, and what type of documentation they had to support CACs. Because some of the TAs did not maintain sufficient documentation, and some TAs who had sponsored contractors had left Korea, we had to obtain a large amount of supporting documentation from the USFK Office of the FKAQ. This office is responsible for reviewing contracts to determine whether they qualify under the Invited Contractor and Technical Representative Program as discussed in USFK Regulation 700-19.

We provided the Social Security numbers of the contractors in our sample to a DoD IG security officer and a security officer with USFK, who reviewed information in JPAS to determine whether the required NACI background investigations on the contractors had been initiated.

Because the DoD IG issued Report D-2009-005 on controls over the CAC life cycle during our audit, we also reviewed the findings, recommendations, and management comments in that report; we discussed these in our report where appropriate.

Use of Computer-Processed Data

We relied on DMDC to extract data from CVS and DEERS to identify contractors who obtained CACs in Korea. We did not perform a formal reliability assessment of the computer-processed data. However, we did validate computer-processed data based on documentation obtained from contracting personnel, TAs, and TASMs in Korea and concluded the data used were reliable. We did not find significant errors between the computer-processed data and source documents that would preclude use of the computer-processed data or change our audit conclusions. However, as previously discussed, we had to remove some individuals from the audit universe because they did not fall within the scope of our audit.

Use of Technical Assistance

We obtained assistance from the DoD IG Quantitative Methods and Analysis Division. The Quantitative Methods and Analysis Division assisted in drawing a sample from a universe of contractors whose CAC cards were issued in Korea. However, we are unable to project from the sample to the universe because the original universe contained individuals and contractors who were out of the audit scope, as previously discussed.

Prior Coverage

During the last 5 years, the Government Accountability Office, the DoD IG, the Naval Audit Service, and the Air Force Audit Agency have issued several reports discussing CACs. Unrestricted Government Accountability Office reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports. Naval Audit Service reports are not available over the Internet. Air Force Audit Agency reports can be accessed from .mil domains over the Internet at https://wwwd.my.af.mil/afknprod/ASPs/cop/Entry.asp?Filter=OO by those with Common Access Cards who create user accounts.

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

DoD IG

DoD IG Report No. D-2009-005, "Controls Over the Contractor Common Access Card Life Cycle," October 10, 2008

DoD IG 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

> This was a summary report based on 14 reports from bases. One of those 14 base reports was for the 51st Fighter Wing at Osan Air Base, Korea.
> Report No. F2008-0011-FBP000, "Contractor Identification Access Controls," February 27, 2008

Air Force Audit Report No. F 2007-0010-FB4000, "Air Force Use of Common Access Card for Physical Access," August 24 2007

> This was a summary report based on three base-level reports and audit work at 12 Air Force installations.

Defense Manpower Data Center Comments

DEPARTMENT OF DEFENSE
HUMAN RESOURCES ACTIVITY
DEFENSE MANPOWER DATA CENTER
1600 WILSON BOULEVARD SUITE 400
ARLINGTON VA 22209-2593

APR 09 2009

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Comments on Draft Report on Controls Over the Contractor Common Access Card Life Cycle in the Republic of Korea (Project No. D2007-D000LA-0199.003)

Thank you for the opportunity to review and provide comments on the draft report "Controls Over the Contractor Common Access Card Life Cycle in the Republic of Korea," Project No. D2007-D000LA-0199.003, dated March 13, 2009.

We agree with the findings and recommendations outlined for the Defense Manpower Data Center (DMDC). Our comments on the draft report and its recommendations are included in attachments 1 and 2. Please feel free to direct any questions to [redacted], or by email at [redacted]

Mary M. Snavely-Dixon
Director

Attachments:
As stated

cc:
Deputy Under Secretary of Defense for Personnel and Readiness (Program Integration)
Director, Defense Human Resource Activity

Attachment 1: **Defense Manpower Data Center (DMDC) Comment to DoD IG Draft Report "Controls Over the Contractor Common Access Card Life Cycle in the Republic of Korea" (Project No. D2007-D000LA-0199.003)**

Recommendations Requiring DMDC Comment:

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

a. Modify the Contractor Verification System to prohibit Trusted Agent Security Managers and Trusted Agents from using the system if they have not taken the required certification training.

b. Clarify the Real-Time Automated Personnel Identification System User Guide by listing eligibility requirements that contractors must meet for the Identification and Privilege Common Access Card and the Geneva Conventions Common Access Card.

c. Clarify the Contractor Verification System User Guide to help a Trusted Agent determine whether or not a Common Access Card or a base pass should be issued to a contractor who needs physical access to Government facilities for short periods."

DMDC Response to Recommendation 2:

2.a. DMDC concurs with this recommendation. Between April and August 2009, DMDC will require existing operators to complete certification training; after a 30-day warning period, TAs/TASMs who have not completed training will be locked out of their CVS accounts.

2.b. DMDC concurs with this recommendation. As of 19 March 2009, the RAPIDS 7.4 User Guide includes updates to clarify both eligibility and documentation requirements for contractors.

2.c. DMDC concurs with this recommendation. In coordination with Defense Human Resource Activity (DHRA), DMDC will update the CVS user guide to improve the understanding of CAC eligibility by August 2009.

Final Report Reference

Attachment 2: Defense Manpower Data Center (DMDC) Remarks on Specific Areas of DoD IG Draft Report "Controls Over the Contractor Common Access Card Life Cycle in the Republic of Korea" (Project No. D2007-D000LA-0199.003)

Item #1 (Section "Previous Audit Findings and Recommendations," Page 2)
Excerpts: "Overall, the CAC life-cycle weaknesses found posed a ***potential national security risk*** that could allow unauthorized access to DoD resources, installations, and sensitive information."
CLARIFICATION: The use of this term is a carry over from DoD IG Report D-2009-005, "Controls Over the Contractor Common Access Card Life Cycle," that mischaracterizes the findings of the audit. All specific references or examples of "potential national security risk" were not directly related to the CAC. The CAC is solely an identification credential that alone should not provide cardholders access to DoD networks or facilitates. The "potential risk" was identified in lack of rapid electronic authentication of credentials and determination of specific needs to have access in the local installation and application owner processes/procedures. Additionally, a specific example cited involved e-mail addresses contained within the PKI certificates of CACs not conforming to DoDI 8500.2. This example gave the impression that the e-mail address within the CAC could allow an individual access to assets; however, the e-mail address has no technical function in the CAC-PKI based website authentication, network authentication, e-mail signing, or e-mail encrypting. The contractor and foreign national designation requirement within DoDI 8500.2 is assigned to network administrators who establish and manage networks and e-mail accounts. Based on the above, we believe the report lacks the foundational basis to use the term "national security risk" in this context concerning the CAC and should be removed from the report.

Item #2 (Section "Contractor Background Investigations," Page 9)
Excerpts: "Of the 177 contractors in our sample, ***50 obtained CACs without the initiation of the required background investigation*** …To determine whether the required background investigation had been initiated for the contractors in our sample, ***we used the Joint Personnel Adjudication System (JPAS),*** that provides real-time information regarding security clearances, access, and investigative status."
CLARIFICATION: The use of JPAS alone to verify background investigations for the sampling of contractors fails to account for all of the systems that contain suitability determination information for contract support personnel. JPAS does not contain suitability information for individuals who do not require access to classified information as well as many individuals of the National Industrial Security Program (NISP).

Revised, page 8

Item #3 (Section "CAC Revocation and Recovery," Page 13)
Excerpts: "Of the CACs issued to contractors in our sample, 168 were terminated. DMDC verified that 112 of these CACs had been recovered and returned to DMDC. Of 56 CACs not returned, only 4 were coded as lost."

Page 11

Final Report Reference

CLARIFICATION: This section implies that DMDC can account for 100% of those cards that have been physically returned. This is not the case, because of the number of returned cards that are no longer functional, worn beyond recognition, or returned between database cycling periods. We recommend adding the following to the report:

A. In areas that discuss cards not returned to DMDC, change the text to "potentially not returned to DMDC."
B. Add a footnote to these areas that states, "Although DoD can account for a majority of the cards that have been physically returned to DMDC for disposal, we cannot account for 100% due to the inherent number of returned cards that are no longer functional or worn beyond recognition."

Information added to clarify (see page 12)

Item #4 (Appendix 1, Page 18)

Excerpts: "We provided the Social Security numbers of the contractors in our sample to a DoD IG security officer and a security officer with USFK, who reviewed information in JPAS to determine whether the required NACI background investigations on the contractors had been initiated."

CLARIFICATION: Same as item #2

Page 17

Inspector General
Department of Defense