

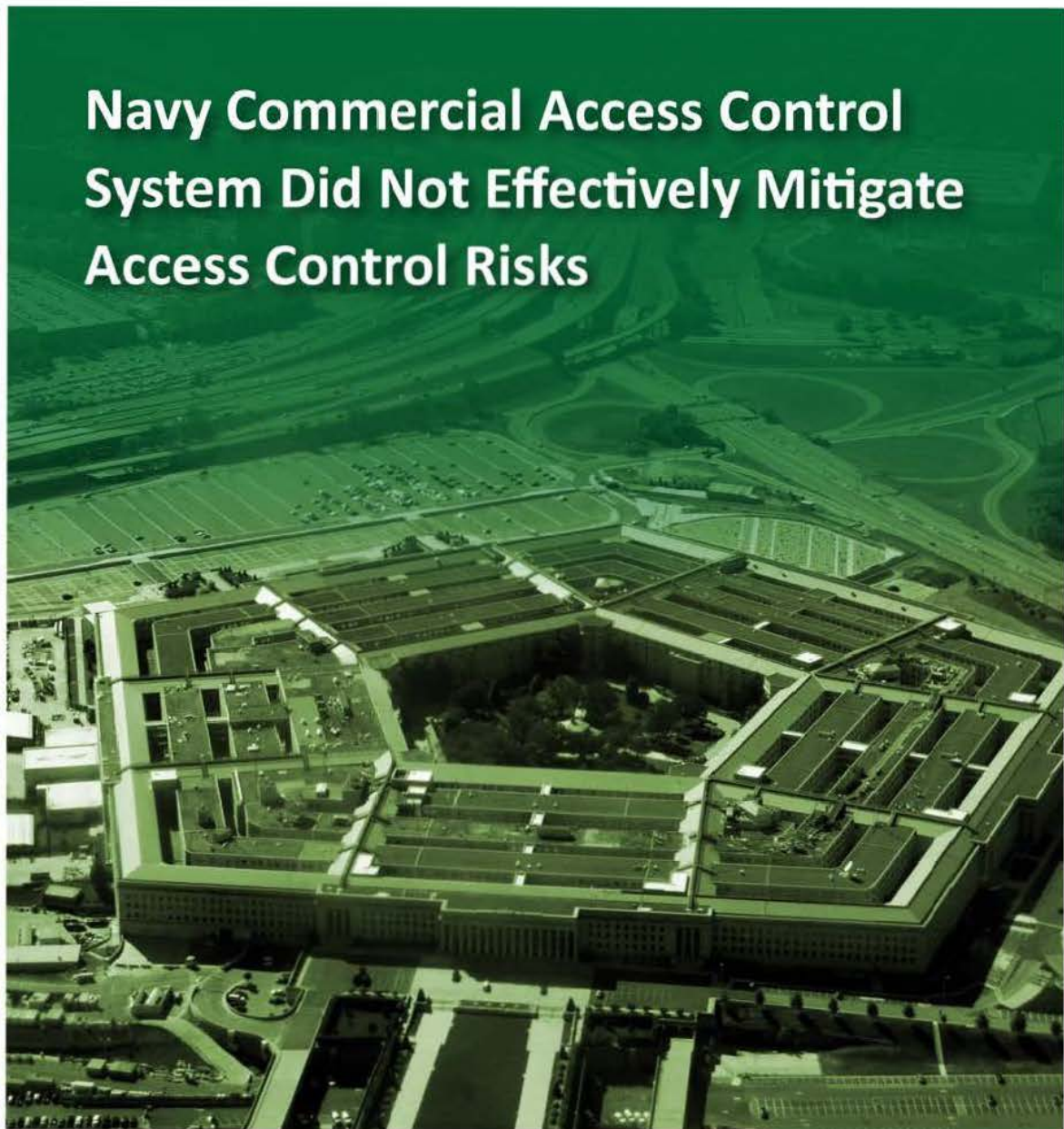
FOR OFFICIAL USE ONLY



INSPECTOR GENERAL

U.S. Department of Defense

SEPTEMBER 16, 2013



Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

FOR OFFICIAL USE ONLY

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that: supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the federal government by leading change, speaking truth, and promoting excellence; a diverse organization, working together as one professional team, recognized as leaders in our field.

.....
Fraud, Waste and Abuse
HOTLINE
1.800.424.9098 • www.dodig.mil/hotline
.....



Results in Brief

Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks

September 16, 2013

Objective

We determined whether the Navy Commercial Access Control System (NCACS) was mitigating access control risks for Navy installations.

Findings

NCACS did not effectively mitigate access control risks associated with contractor installation access. This occurred because Commander, Navy Installations Command (CNIC) officials attempted to reduce access control costs. As a result, 52 convicted felons received routine, unauthorized installation access, placing military personnel, dependents, civilians, and installations at an increased security risk. Additionally, the CNIC N3 Antiterrorism office (N3AT) misrepresented NCACS costs. This occurred because CNIC N3AT did not perform a comprehensive business case analysis and issued policy that prevented transparent cost accounting of NCACS. As a result, the Navy cannot account for actual NCACS costs, and DoD Components located on Navy installations may be inadvertently absorbing NCACS costs. Furthermore, CNIC N3AT officials and the Naval District Washington Chief Information Officer circumvented competitive contracting requirements to implement NCACS. This occurred because CNIC N3AT did not have contracting authority. As a result, CNIC N3AT spent over \$1.1 million in disallowable costs and lacked oversight of, and diminished legal recourse against, the NCACS service provider.

Recommendations

We recommend CNIC replace Rapidgate with a system that uses the mandatory databases and revise CNIC policy and guidance to align with Federal and DoD credentialing requirements. Furthermore, we recommend CNIC establish a process to identify and provide commanders with resources and capabilities to access required authoritative databases.

Additionally, we recommend the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), obtain an independent, comprehensive business case analysis of NCACS and determine future actions for contractor installation access. We also recommend the Director perform a review of CNIC N3AT officials and consider administrative actions, if appropriate. We also recommend the Assistant Secretary of the Navy (Research, Development, and Acquisition), review the inappropriate contracting practices and establish a corrective action plan.

Comments

Comments submitted for CNIC were nonresponsive regarding the recommendations to replace Rapidgate with a system that uses the mandatory databases, revise CNIC policy, and provide installations with resources to access the mandatory databases. The Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), comments were generally responsive. However, the Director's comments were partially responsive regarding the review of CNIC N3AT officials. Comments submitted for the Assistant Secretary of the Navy (Research, Development, and Acquisition) were responsive. We request management provide additional comments by October 18, 2013. See the Recommendations Table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Assistant Secretary of the Navy (Research, Development, and Acquisition)		B.1, C.1, C.2
Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics)	C.3.a, C.3.b, C.3.c	B.2.a, B.2.b
Commander, Navy Installations Command	A.1, A.2, A.3.a, A.3.b	
Director of Contracts, Naval Sea Systems Command		C.2
Chief of Contracting, Naval Surface Warfare Center, Panama City		C.4.a, C.4.b
Chief of Contracting, Naval Surface Warfare Center, Port Hueneme		C.4.a, C.4.b

Please provide comments by October 18, 2013.



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

September 16, 2013

MEMORANDUM FOR ASSISTANT SECRETARY OF THE NAVY (RESEARCH,
DEVELOPMENT, AND ACQUISITION)
DIRECTOR, SHORE READINESS, DEPUTY CHIEF OF NAVAL
OPERATIONS (FLEET READINESS AND LOGISTICS)
COMMANDER, NAVY INSTALLATIONS COMMAND
DIRECTOR OF CONTRACTS, NAVAL SEA SYSTEMS COMMAND
CHIEF OF CONTRACTING, NAVAL SURFACE WARFARE CENTER,
PANAMA CITY
CHIEF OF CONTRACTING, NAVAL SURFACE WARFARE CENTER,
PORT HUENEME

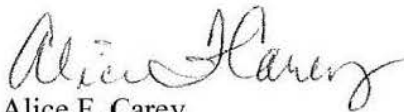
SUBJECT: Navy Commercial Access Control System Did Not Effectively Mitigate Access Control
Risks (Report No. DODIG-2013-134)

We are providing this report for your review and comment. The Navy Commercial Access Control System (NCACS) did not effectively mitigate contractor access control risks and allowed convicted felons to access Navy installations without the knowledge and approval of the installation commander. In addition, Commander, Navy Installations Command, N3 Antiterrorism office, misrepresented NCACS costs and circumvented competitive contracting requirements to implement NCACS. We considered management comments on a draft of this report from the Department of the Navy, through the consolidated responses by the Deputy Under Secretary of the Navy (Plans, Policy, Oversight, and Integration), when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Comments submitted for the Assistant Secretary of the Navy (Research, Development, and Acquisition); Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics); and Director of Contracts, Naval Sea Systems Command, were generally responsive. Comments submitted for the Commander, Navy Installations Command were nonresponsive. We request the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), provide additional comments on Recommendation C.3 and the Commander, Navy Installations Command, provide additional comments on Recommendations A.1, A.2, and A.3 by October 18, 2013.

If possible, send a Microsoft Word (.doc) file and portable document format (.pdf) file containing your comments to audros@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 me at (703) 604-[REDACTED] (DSN 664-[REDACTED]).


Alice F. Carey
Assistant Inspector General
Readiness, Operations, and Support

Contents

Introduction

Objective	1
Background	1
Review of Internal Controls	4

Finding A. NCACS Did Not Effectively Mitigate Access Control Risks for Contractors Entering Navy Installations

Requirements to Vet Contractors Accessing Navy Installations	5
Contractor Employees Enrolled in Rapidgate Received Interim Installation Access Without a Background Check	6
Contractor Employees Received Credentials Without Being Vetted Through Authoritative Databases	7
CNIC Attempted to Reduce Access Control Costs	9
Installation Personnel Did Not Have Appropriate Resources to Conduct Background Checks	10
Military and Civilian Personnel Placed at Security Risk	11
Naval Criminal Investigative Services Concerned with Accuracy and Reliability of Rapidgate	13
Management Comments on the Report	13
Recommendations, Management Comments, and Our Response	14

Finding B. NCACS Projected Costs Not Supported

Costs Not Identified or Properly Represented	18
CNIC Cost Claims Unreliable and Unsubstantiated	19
NCACS Costs are Unknown	20
Recommendations, Management Comments, and Our Response	21

Finding C. CNIC Circumvented Competitive Contracting Requirements

Contractor Competition is Required	23
Rapidgate Procurement History	23
Prime Contractor Directed to Enter Into Unauthorized Commitments	24

CNIC Officials' Actions Restricted Full and Open Competition	26
Navy Lacks Contractual Coverage for Eid Passport Services	26
Appropriate Contracting Authority Was Not Used	27
Navy Spent Over \$1.1 Million in Potentially Unallowable Costs and Lacked Oversight and Legal Recourse Against Eid Passport	28
Conclusion	28
Recommendations, Management Comments, and Our Response	29

Appendixes

Appendix A. Scope and Methodology	32
Use of Computer-Processed Data	33
Prior Coverage	33
Appendix B. Identified Contractor Companies and Amounts Charged for NCACS-Related Costs	35

Glossary	36
-----------------	----

Management Comments

Department of the Navy Comments	38
---------------------------------	----

Acronyms and Abbreviations	45
-----------------------------------	----



Introduction

Objective

The objective of the audit was to determine whether the Navy Commercial Access Control System (NCACS) is mitigating access control risks to Navy installations. See Appendix A for a discussion of the scope and methodology and prior audit coverage.

Background

NCACS Overview

NCACS is an enterprise identity management and perimeter installation access control solution used to manage commercial vendors, contractors, and suppliers¹ requiring routine access to Navy installations. NCACS was implemented by the Commander, Navy Installations Command (CNIC), the office designated to oversee the physical security of all Continental United States Navy installation perimeters. NCACS is managed by the CNIC N3 Antiterrorism office (N3AT) and administered through a service provider, Eid Passport, Incorporated (Eid Passport). Eid Passport used its access control system, known as Rapidgate,² to provide NCACS services. Eid Passport was designated the responsibility to perform contractor background checks, manufacture Rapidgate credentials, and maintain information on contractors enrolled in Rapidgate accessing Navy installations. The Rapidgate credential provided the contractor with unescorted, recurring installation access.

Navy Contractor Credentialing

Chief of Naval Operations Instruction (OPNAVINST) 5530.14E, "Navy Physical Security and Law Enforcement Program," January 28, 2009, change 1, April 19, 2010, directs elimination of local credentials but allowed supplemental credentialing systems to be used as an additional level of access control security not presently afforded by the Common Access Card.

In July 2010, CNIC issued Notice³ 5530, "RAPIDGate Implementation for Non-Common Access Card (CAC) Contractors/Vendors Program Within CONUS Regions, Navy Region Hawaii and Joint Region Marianas," to implement Rapidgate as the standard identity management and perimeter installation access control solution for contractors not

¹ For the purpose of this report, commercial vendors, contractors, and suppliers will be referred to as "contractors."

² "RAPIDGate" is a registered trademark of Eid Passport, Incorporated.

³ According to the OPNAVINST 5215.17, "Navy Directives Issuance System," June 13, 2005, a notice is a directive that has a one-time or brief nature and is not permitted to remain in effect for longer than 1 year.

authorized a Common Access Card. In order to avoid the appearance of endorsing Rapidgate, Eid Passport's trademarked product, in May 2011, CNIC updated and issued Notice 5530, to rename its standard installation access control solution to NCACS. In July 2012, CNIC updated and issued Notice 5530, which identifies acceptable forms of identification for contractors requiring physical access to Navy installations, including:

- Federal and DoD-issued credentials, including the Personal Identity Verification (PIV) credential or Transportation Worker Identification Card,
- Rapidgate credentials, and
- Local installation passes.

According to CNIC Notice 5530, contractors not authorized to receive a Federal or DoD issued credential could request participation in the Navy's NCACS program to obtain a Rapidgate credential. If a contractor employee elects not to participate in NCACS, the individual employee may apply for a locally issued pass providing 1 day of installation access. Each individual employee applying for a locally issued daily pass must be processed through the installation Pass and Identification office, present valid forms of identification, and undergo required background vetting by installation security personnel.

Rapidgate Enrollment Process

NCACS is a voluntary program that allowed contractors recurring installation access. To enroll in Rapidgate, the contractor company is required to obtain verification from a designated NCACS installation sponsor. Once verified and approved, the contractor company then pays Eid Passport an enrollment fee of \$199 annually for access to a single installation, or \$249 annually for access to multiple installations. If the contractor employee chooses to participate in NCACS, the employee registers at a Rapidgate kiosk for installation access. Eid Passport requires an additional enrollment fee for each contractor employee that registers for Rapidgate. An employee can receive a Rapidgate credential that provides installation access for 90 days or 1 year for the following enrollment fees:

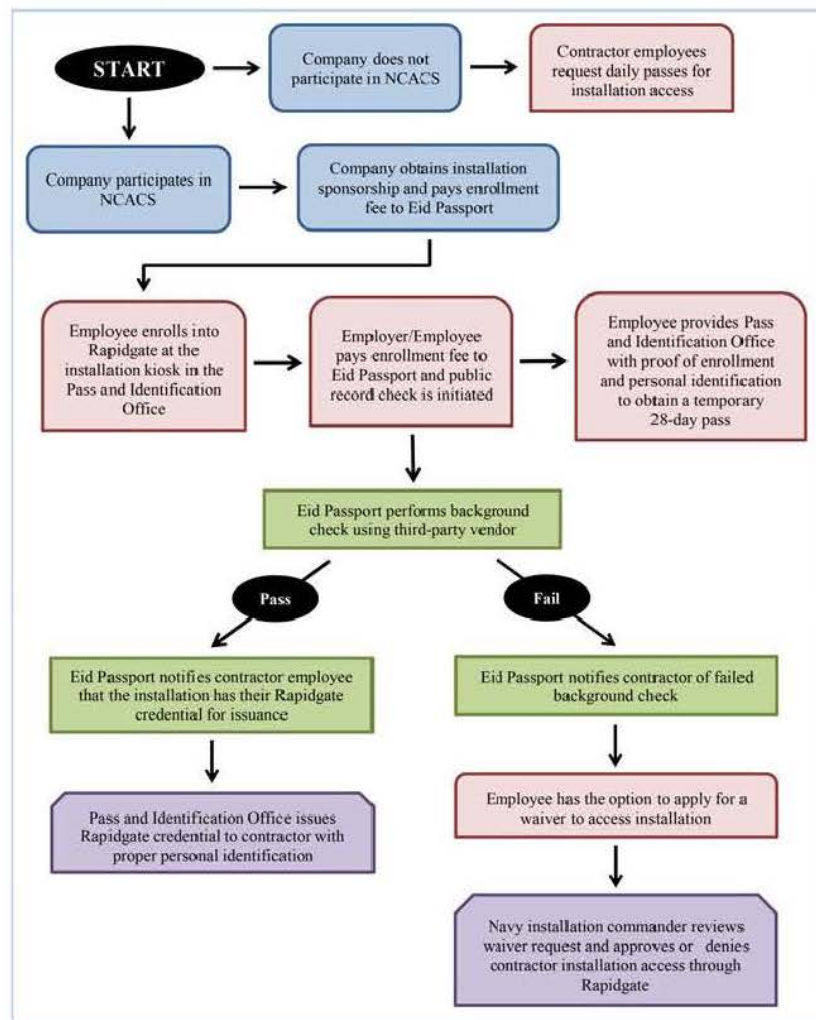
- \$159 for 1 year of access to a single installation,
- \$199 for 1 year of access to multiple installations, or
- \$59 for 90 days of access to a single installation.

After receiving the contractor employee's enrollment fee, Eid Passport's third-party vendors perform public record checks using publicly accessible databases. However,

Eid Passport stated, "not all public records are up-to-date, complete, accurate, or available." Before the public record checks are completed, contractor employees enrolled in Rapidgate can obtain temporary installation access for up to 28 days. Contractor employees present the installation's Pass and Identification Office with a Rapidgate enrollment receipt and personal identification to obtain interim access until they are authorized or denied participation in Rapidgate.

After Eid Passport determines the contractor employee passed the public record check, it provides the installation(s) with the employee's Rapidgate credential for issuance. The Rapidgate credential is valid for up to 5 years but only remains active for up to 1 year at a time. To keep the Rapidgate credential active for another year, Eid Passport requires contractor employees to pay an annual fee and undergo a renewal background check. In addition to the renewal background checks, contractor employees are also subject to periodic public record checks. These periodic checks search limited public records for changes in the employee's criminal history since the previous background check. However, if Eid Passport determines the contractor employee failed the public record check, the employee has the option to submit a waiver request to the installation commanding officer. The commanding officer reviews the waiver request and failed public record check to determine whether the installation accepts the risk of granting the contractor employee installation access. If the commanding officer accepts the associated risk, the employee can participate in NCACS and is granted a Rapidgate credential allowing unescorted access to the installation. If the commanding officer does not accept the risk, the contractor employee cannot participate in NCACS. See Figure 1 on page 4 for a diagram of the NCACS participation process.

Figure 1. NCACS Participation Process



Review of Internal Controls

DoD Instruction 5010.40, “Managers’ Internal Control Program Procedures,” May 30, 2013, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses for the Navy. In attempt to reduce access control costs, CNIC did not follow Federal credentialing standards and DoD contractor vetting requirements and did not provide 7 of the 10 installations visited the appropriate resources and capabilities to conduct required contractor background checks. Furthermore, CNIC N3AT did not perform a comprehensive business case analysis (BCA) and issued policy that prevented transparent accounting for actual NCACS costs. Additionally, CNIC N3AT did not have contracting authority and developed a certification of compliance (COC) as an administrative approach to maintain a relationship with Eid Passport. We will provide a copy of the report to the senior Navy official responsible for internal controls.

Finding A

NCACS Did Not Effectively Mitigate Access Control Risks for Contractors Entering Navy Installations

The Navy Commercial Access Control System, Rapidgate, did not effectively mitigate the access control risks of contractors accessing Navy installations. Specifically, numerous contractor employees enrolled in Rapidgate received interim installation access and Rapidgate credentials without having their identities vetted through mandatory authoritative databases, such as the National Crime Information Center (NCIC) database and the Terrorist Screening Database. Furthermore, as an alternative to NCACS, contractor employees could obtain a local daily pass without having their identities vetted through NCIC and the Terrorist Screening Database. This occurred because—in an attempt to reduce access control costs—CNIC did not:

- follow Federal credentialing standards and DoD contractor vetting requirements and
- provide 7 of the 10 installations visited with the appropriate resources and capabilities to conduct required contractor background checks.

As a result, 52 convicted felons received routine, unauthorized access to Navy installations for 62 to 1,035 days since Eid Passport's initial public record checks did not identify the felony convictions. This placed military personnel, dependents, civilians, and installations at an increased security risk.

Requirements to Vet Contractors Accessing Navy Installations

Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004, requires that all Government employees and contractors who require routine physical access to Government facilities and installations receive a standard and secure identification credential. In accordance with Homeland Security Presidential Directive 12, the Department of Commerce's National Institute of Standards and Technology issued the Federal Information Processing Standard 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors," change notice 1, March 2006, which identifies the PIV credential as the standard Federal identification credential. The PIV credential is a secure identification credential that Federal employees and contractors can use to

gain access to federally controlled facilities and installations. According to Office of Management and Budget Memorandum 05-24, "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," August 5, 2005, (OMB Memorandum 05-24), Government employees and contractors requiring routine physical access to an installation for greater than 6 months must receive a PIV credential.

DoD Directive Type Memorandum (DTM) 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009, incorporating change 3, March 19, 2013, establishes identity vetting standards across DoD. DTM 09-012 aligns with Federal vetting standards to require that PIV-eligible contractors receive a National Agency Check with Written Inquiries background investigation prior to determining fitness. DTM 09-012 requires that contractors without a Federal PIV or DoD-issued credential⁴ be vetted through NCIC and the Terrorist Screening Database to gain unescorted access to DoD installations and stand-alone facilities. According to DTM 09-012, these access control standards shall be implemented as resources, law, and capabilities permit.

Contractor Employees Enrolled in Rapidgate Received Interim Installation Access Without a Background Check

CNIC policy provided contractor employees enrolled in Rapidgate interim installation access before a background check was completed. CNIC Notice 5530 allows contractors who registered with NCACS at the installation's Rapidgate kiosk, without a completed background check, to obtain temporary installation access for up to 28 days. For example, 9 of the 10 Navy installations visited allowed temporary access to contractor employees enrolled in Rapidgate prior to completing a background check. According to installation security personnel, after registration at the installation's Rapidgate kiosk, contractor employees were only required to present a Rapidgate enrollment receipt to qualify for 28 days of unescorted access. However, the employee's claimed identity was not vetted against mandatory authoritative databases. By giving contractors interim installation access before vetting them through the mandatory authoritative databases, the NCACS process and CNIC Notice 5530 violated DTM 09-012.

⁴ A DoD-issued credential includes the Common Access Card.

Contractor Employees Received Credentials Without Being Vetted Through Authoritative Databases

Eid Passport vetted contractor employees enrolled in Rapidgate through the use of public record checks. DTM 09-012 requires an authorized Government representative to conduct identity-proofing and vetting of a claimed identity to determine an individual's fitness for installation access. Only personnel delegated by the installation commander shall perform access control duties, including identity proofing, vetting and determination of fitness, and access authorization and privileges. However, CNIC policy appointed Eid Passport to manage the NCACS program through Rapidgate and determine the fitness of contractor employees for installation access. CNIC delegated to Eid Passport the responsibility to collect the contractor employee's enrollment information and vet the employee through public record databases. After Eid Passport determined the contractor employee passed the public record check, Eid Passport provided Navy installations with the employee's Rapidgate credential for issuance. Navy installation officials relied on Eid Passport's adjudication of contractor employees and only validated an employee's identity through proof of ID, such as a driver's license, and proof of employment to issue the Rapidgate credential.

In addition, the public record databases used by Eid Passport were unreliable. Eid Passport acknowledged, "neither the Service Provider nor its screening providers can guarantee the completeness or accuracy of the data obtained," and the results of the checks were subject to the reliability of the public records searched, which were not always up-to-date. CNIC N3AT officials approved the Rapidgate Statement of Work and knowingly accepted the security risks associated with the accuracy and reliability issues of the public record checks. CNIC N3AT officials stated performing public record checks through Rapidgate improved the Navy's previous physical access controls, which did not include any contractor background checks. Furthermore, CNIC Notice 5530 states that an NCACS objective is to enhance installation safety and security. However, due to the unreliable accuracy of vetting contractors through the Rapidgate system, the claimed reductions in security risk provided installation commanders with a false sense of security, leaving installations exposed to potentially hostile actions.



Eid Passport acknowledged, "neither the Service Provider nor its screening providers can guarantee the completeness or accuracy of the data obtained,"

~~(FOUO)~~ Furthermore, contractor employees obtained Rapidgate credentials that were active for 1 year, regardless of the length of time a contractor required installation access. According to OMB Memorandum 05-24, Government employees and contractors

~~(FOUO)~~ requiring routine physical access to an installation for greater than 6 months must receive a PIV credential. To obtain a PIV credential, the employee, at a minimum, must undergo a National Agency Check with Written Inquiries background investigation. The investigation provides the Government with assurance that an individual meets the fitness requirements for accessing federally controlled facilities. However, once a contractor employee enrolled in Rapidgate passed the initial Eid Passport public record check and paid the associated 1-year fee, the employee received unescorted installation access for 1 year. For example, a [REDACTED] contractor was required to perform deliveries on the installation with a service period of approximately 1 year. To obtain installation access, the contractor's employees participated in NCACS and received Rapidgate credentials. However, the employees required routine physical access for greater than 6 months and should have received PIV credentials with the subsequent background investigations, as required by OMB Memorandum 05-24.

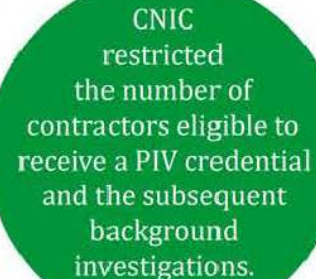
~~(FOUO)~~ Additionally, seven Navy installations granted access to contractor employees without vetting employee identities through NCIC and the Terrorist Screening Database. DTM 09-012 requires that contractors without a Federal PIV or DoD-issued credential be vetted through the NCIC database and the Terrorist Screening Database to gain unescorted access to DoD installations and stand-alone facilities. According to DTM 09-012, these vetting standards shall be implemented as resources and capabilities permit. Of 10 installations visited, 7 Navy installations did not vet all contractor employees through NCIC before issuing Rapidgate credentials and daily passes. For example, [REDACTED] only performed local database searches to vet contractor employees obtaining daily passes. Local databases used by installations included Sex Offender Registration and Notification Act and local no-entry lists. Contractor employees obtaining Rapidgate credentials to access the installation received the public record checks performed by Eid Passport's third-party vendor. However, none of the contractor employees entering the installation were vetted against NCIC and the Terrorist Screening Database, as required.

~~(FOUO)~~ The remaining three installations vetted all contractor employees through the NCIC database before issuing Rapidgate credentials and daily passes. For example, [REDACTED], had the capability to access NCIC through the Navy Region Mid-Atlantic Security Office and required all contractor employees accessing the installation to undergo an NCIC check before issuing a Rapidgate credential or a daily pass. Navy Region Mid-Atlantic Security Office personnel stated that, using NCIC, they identified contractors with felony charges not found by the Rapidgate public record checks and denied access to these contractor employees. If the installation solely relied on the public record checks, these contractors would have otherwise been granted a Rapidgate credential that facilitated unescorted installation access.

CNIC Attempted to Reduce Access Control Costs

CNIC attempted to reduce its access control costs through NCACS. According to a Navy instruction, CNIC is responsible for providing the support and funding for the physical security of Navy installations. To reduce CNIC's physical security costs, CNIC increased contractor participation in NCACS by issuing NCACS policy that did not follow Federal contractor employee credentialing and vetting requirements.

According to OMB Memorandum 05-24, Government employees and contractors requiring routine physical access to an installation for greater than 6 months must receive a PIV credential and undergo a National Agency Check with Written Inquiries background investigation. However, CNIC's NCACS implementation policy included additional access requirements for contractor PIV credential eligibility and increased the number of contractors eligible to receive a Rapidgate credential. According to CNIC Notice 5530,



CNIC restricted the number of contractors eligible to receive a PIV credential and the subsequent background investigations.

a contractor must require both physical access to a Navy installation and logical access to a Navy or DoD network to be eligible to receive a DoD PIV credential. Since CNIC included the requirement for contractors to require logical access to receive a PIV credential, CNIC restricted the number of contractors eligible to receive a PIV credential and the subsequent background investigations.

By restricting PIV credential eligibility requirements, CNIC increased the number of contractors eligible to receive a Rapidgate credential and minimized CNIC's costs to perform contractor credentialing and vetting. According to CNIC Notice 5530, contractors determined by CNIC to be ineligible for a PIV credential can only gain reoccurring installation access by participating in NCACS. Contractors participating in NCACS must pay Eid Passport to perform background vetting and create Rapidgate credentials. Additionally, the Rapidgate Statement of Work states that contractors who participate in NCACS are only vetted using public record checks to obtain unescorted installation access. CNIC should discontinue the use of Rapidgate and any other system that exclusively uses publicly available databases to vet and adjudicate contractor employees accessing Navy installations and implement a system that meets Federal and DoD requirements for background vetting using the mandatory databases. Additionally, CNIC should revise NCACS policy to align with Federal and DoD contractor vetting and credentialing requirements to provide contractors with the required credentials and background investigations.

Installation Personnel Did Not Have Appropriate Resources to Conduct Background Checks

CNIC did not provide 7 of 10 Navy installations visited the appropriate resources and capabilities to conduct mandatory NCIC and Terrorist Screening Database checks. DoD DTM 09-012 requires contractors without a Federal PIV or DoD-issued credential to be vetted through authoritative databases before granting unescorted installation access, as resources and capabilities permit. DTM 09-012 states installation Government representatives must query NCIC and the Terrorist Screening Database to vet and determine the fitness of a contractor employee. According to a Navy instruction, CNIC is responsible for providing the support and funding for the physical security of Navy installations.

~~(FOUO)~~ Of the 10 Navy installations visited, 7 did not have access to NCIC and the Terrorist Screening Database to properly vet all contractor employees. CNIC N3AT officials stated that they provided installations funding to perform NCIC and Terrorist Screening Database checks. However, installation security personnel stated the installations lacked the resources or capability to conduct NCIC and Terrorist Screening Database checks on all contractor employees. For example, installation security personnel at [REDACTED], stated they did not have the resources to screen every contractor employee through NCIC before issuing a Rapidgate credential or daily pass. The installation also did not have the capability to access the NCIC database. Additionally, installation security personnel at [REDACTED], did not have the capability to access NCIC. Specifically, personnel stated that they did not have NCIC terminals at the installation to connect to the NCIC database. See Table 1 on page 11 for an installation breakdown of contractor vetting through NCIC and the Terrorist Screening Database. CNIC should provide the seven installations identified with the resources and capabilities to access NCIC and the Terrorist Screening Database to vet contractors requesting access to Navy installations. Furthermore, CNIC should establish a process to identify which remaining Navy installations need resources and capabilities to conduct NCIC and Terrorist Screening Database checks before granting contractor employees installation access.

~~(FOUO)~~ Table 1. Installation Contractor Vetting Through NCIC and the Terrorist Screening Database

Installations Visited	Vets All Contractors	Does Not Vet All Contractors	
		Lacked Resources	Lacked Capability
[REDACTED]			X
[REDACTED]			X
[REDACTED]	X		
[REDACTED]		X	X
[REDACTED]			X
[REDACTED]		X	
[REDACTED]	X		
[REDACTED]	X		
[REDACTED]		X	X
[REDACTED]			X

Military and Civilian Personnel Placed at Security Risk

There were 52 convicted felons who received routine access to Navy installations even though their felony convictions occurred before they were issued a Rapidgate credential. This placed military personnel, dependents, civilians, and installations at an unacceptable level of safety and security risk. Although CNIC N3AT officials claimed NCACS increased installation security over the previous approach of providing no contractor employee background checks, NCACS provided installation commanders with a false sense of security. Contractor employees with prior felony convictions received Rapidgate credentials without the knowledge and approval of the installation commander. Eid Passport public record checks showed that 53 individuals failed a renewal or periodic check. Of the 53 public record checks, 52 contractor employees were allowed installation access before Eid Passport identified their felony convictions, even though their felony convictions occurred before the contractor was issued a Rapidgate credential. The felony convictions were not identified during the initial Rapidgate public record checks, even though the felonies identified occurred an average of 13 years prior to passing the initial Rapidgate screening. The remaining public record check was a renewal check that identified the individual had a

There were 52 convicted felons who received routine access to Navy installations.

Social Security Number that was invalid, belonged to a deceased person, was listed in a True Name Fraud Alert, or belonged to another individual. However, this Social Security Number issue was not identified on the initial Eid Passport public record check, and the individual had installation access for 345 days before this issue was identified. In every CNIC region we visited, we identified contractors enrolled in Rapidgate who were given installation access before felony convictions were identified. See Table 2 for a regional breakdown.

Table 2. Rapidgate Contractors Accessing Navy Installations with Previously Unidentified Felonies

CNIC Navy Region	Number of Installations Visited	Rapidgate Contractors with Previously Unidentified Felonies Accessing Installations Visited
Navy District Washington	2	1
Mid-Atlantic	2	12
South East	2	8
Midwest	1	15
North West	1	6
South West	2	10
Total	10	52

For example, one contractor employee was first issued a Rapidgate credential in June 2009. According to the public record check performed by Eid Passport’s third-party vendor, the employee failed a Rapidgate renewal check in April 2012, based on a felony conviction for “conspiracy to distribute...cocaine base.” This felony conviction occurred in 2000 but was not identified by Eid Passport’s check until the employee failed the renewal check in April 2012. This contractor employee had unescorted access to a Navy installation for 1,035 days before the felony conviction was identified. Furthermore, another contractor employee was issued a Rapidgate credential in October 2011 and failed a periodic public record check in January 2012. The individual failed the public record check based on a felony conviction of “indecent liberties with a child” that occurred in 1987. Before the felony was identified, the contractor employee had 91 days of unescorted access to a Navy installation. Given that child development centers, schools, and family housing are located on many Navy installations, accurate vetting of contractor employees is essential to ensure the safety of children on Navy installations.

Additional examples of unidentified felony convictions in the public record checks included drug possession, assault, theft, and throwing a missile⁵ at an occupied vehicle. Installation commanding officers were unaware that the Rapidgate system had granted contractor employees with prior felony convictions reoccurring access to their installations. The prior felony convictions should have been identified by the initial public record checks performed on these employees. Instead, the felonies were not identified until subsequent Rapidgate public record checks, such as annual renewals and periodic checks, were performed by Eid Passport's third-party vendors. Therefore, CNIC N3AT provided installation commanders with a false sense of security by knowingly accepting the security risks associated with public record databases that were not all "up-to-date, complete, accurate, or available."

Naval Criminal Investigative Services Concerned with Accuracy and Reliability of Rapidgate

~~(FOUO)~~ According to Naval Criminal Investigative Services Headquarters officials, the Naval Criminal Investigative Services [REDACTED] Field Office expressed concern with the accuracy and reliability of Rapidgate background vetting. The Naval Criminal Investigative Services [REDACTED] Field Office identified multiple criminal incidents, such as convictions for cocaine distribution, associated with Rapidgate contractor background vetting and initiated an inquiry into the Rapidgate operations at the [REDACTED]. Based on the identified incidents, the special agent leading the inquiry contacted SecurTest, one of the third-party background screeners used by Eid Passport. The agent requested that SecurTest provide details on how background vetting is accomplished for non-DoD applicants participating in Rapidgate. According to the special agent, SecurTest allegedly queried the applicants against sex offender registries and Clerk of the Court records in the locations the applicant disclosed to have resided. Thus, according to the special agent, the background vetting is not nationwide and solely relies on the integrity of application information. Naval Criminal Investigative Services [REDACTED] Field Office personnel stated that they plan to run over 3,000 Rapidgate cardholders through NCIC to determine whether any convicted felons were undetected and granted installation access.

Management Comments on the Report

The Department of the Navy, through the Deputy Under Secretary of the Navy (Plans, Policy, Oversight, and Integration), consolidated the management comments from the Director,

⁵ A missile is any object thrown or projected, such as a stone or a bullet.

Program Analysis and Business Transformation and Director, Services Acquisition, Office of the Deputy Assistant Secretary of the Navy (Acquisition and Procurement); Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics); Deputy Commander, Navy Installations Command; and Associate Director of Contracts, Naval Sea Systems Command regarding our recommendations. CNIC requested further discussion on the disposition of Recommendations A.1 – A.3 and Recommendation C.3. We held discussions with CNIC and considered those discussions in the final preparation of our report.

Recommendations, Management Comments, and Our Response

Recommendation A.1.

We recommend the Commander, Navy Installations Command, immediately discontinue the use of Rapidgate and any other system that exclusively uses publicly available databases to vet and adjudicate contractor employees accessing Navy installations, and replace it with a system or process that meets Federal and DoD requirements for background vetting.

Commander, Navy Installations Command Comments

The Deputy Commander, Navy Installations Command, responding for the Commander, Navy Installations Command, disagreed with the recommendation. The Deputy Commander stated NCACS standards meet Federal and DoD requirements for background vetting and that the Navy currently conducts NCIC checks and final credential issuance. Additionally, the Deputy Commander stated that prior to accepting a commercial credential source for NCACS, the credentialing firm must demonstrate full compliance with Federal, DoD, and Navy standards, including DTM 09-012. Finally, the Deputy Commander stated that discontinuing NCACS will ensure long lines at Navy access points, resulting in productivity loss for contractors doing business on Navy installations, and would require hiring additional civil servants to work in base pass offices.

Our Response

Comments from the Deputy Commander, Navy Installations Command, were nonresponsive. NCACS is administered by a commercial credentialing source, Eid Passport, which uses Rapidgate to vet contractor employees accessing Navy installations. As noted in our draft report, Rapidgate relies exclusively on unreliable public record databases. CNIC N3AT's Program Director acknowledged that

Eid Passport does not have the capability to perform NCIC checks, and that Navy installations should be performing an NCIC check prior to providing contractors an NCACS credential. Also, as noted in our draft report, not all installations had access to the NCIC database. Since Eid Passport does not have the capability to perform NCIC checks to vet contractor employees, and not all Navy installations have the ability to access NCIC, NCACS is not fully compliant with DoD background vetting standards outlined in DTM 09-012.

Additionally, the Deputy Commander stated that if NCACS was discontinued, additional civil servants would need to be hired to work at the base pass offices. However, Navy Region Mid-Atlantic successfully used only three full-time employees to administer NCIC screenings for all contractors accessing 15 Navy installations. Navy Region Mid-Atlantic personnel reported that the NCIC checks resulted in the identification of and subsequent denial of installation access for felons not identified by Rapidgate. Therefore, based on Rapidgate's unreliable public record checks, Rapidgate could be eliminated resulting in potential cost savings for the Navy. We request that the Commander, Navy Installations Command, reconsider the recommendation and provide additional comments on the final report.

Recommendation A.2.

We recommend the Commander, Navy Installations Command, revise Instruction 5530.14, "CNIC Ashore Protection Program," July 7, 2011, and Notice 5530, "Navy Commercial Access Control System Within Continental United States Regions, Navy Region Hawaii, and Joint Region Marianas," July 5, 2012, to require contractor employees requiring routine physical access to Navy installations for greater than 6 months receive the DoD Personal Identity Verification credential with the National Agency Check with Written Inquiries.

Commander, Navy Installations Command Comments

The Deputy Commander, Navy Installations Command, responding for the Commander, Navy Installations Command, disagreed with the recommendation. The Deputy Commander stated CNIC is following DoD and congressional guidance to accept identity credentials from non-Federal issuers. The Deputy Commander stated that CNIC's understanding of current policy is that both requirements—physical access to an installation for greater than 6 months and logical access to the Navy's networks—must be met for receipt of a Common Access Card. Additionally, the Deputy Commander stated NCACS vetting combined with the NCIC check encompasses those checks conducted via a National Agency Check with Written Inquiries.




Our Response

Comments from the Deputy Commander, Navy Installations Command, were nonresponsive. If it was the Deputy Commander's intent to indicate compliance with DoD and Congressional guidance by accepting Personal Identity Verification Interoperable (PIV-I) credentials from non-Federal issuers as an alternative to issuing PIV credentials, then we disagree. As noted in our draft report, OMB Memorandum 05-24 states that Government employees and contractors requiring routine physical access to an installation for greater than 6 months must receive a PIV credential. According to the Federal Chief Information Officer Council, "Personal Identity Verification Interoperable Frequently Asked Questions," June 28, 2010, agencies cannot accept PIV-I cards issued by a contractor's company in lieu of issuing PIV cards to those individuals. Specifically, "individuals who fall within the applicability of HSPD-12, including Federal contractors requiring routine access to Federally-controlled facilities or Federally-controlled information systems for a period of time greater than 6 months, must continue to be issued PIV cards by the Federal Government." The Office of Personnel Management issued "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," July 31, 2008, which provides Government-wide PIV credentialing standards for employees and contractor personnel. A senior program analyst, speaking on behalf of the Office of Personnel Management's Federal Investigative Services Division, confirmed that contractor personnel requiring only routine physical access to federally controlled facilities for greater than 6 months are required to be issued a PIV credential. Therefore, CNIC should issue PIV credentials, not Rapidgate credentials, to contractor employees who only require routine physical access to Navy installations for greater than 6 months.

Additionally, the Deputy Commander stated that NCACS vetting combined with the NCIC check encompasses those checks conducted via a National Agency Check with Written Inquiries. However, as noted in our draft report, the public record databases used by Eid Passport were unreliable, and OMB Memorandum 05-24 states employees and contractors must undergo a National Agency Check with Written Inquiries background investigation to obtain a PIV credential. We request that the Commander, Navy Installations Command, reconsider the recommendation and provide additional comments on the final report.

Recommendation A.3.

We recommend, the Commander, Navy Installations Command:

~~(FOUO)~~ a. Provide 



~~(FOUO)~~ [REDACTED], the resources and capabilities needed to access National Crime Information Center and the Terrorist Screening Database.

- b. Establish a process to identify which installations need resources and capabilities to access the National Crime Information Center and the Terrorist Screening Database for contractor background vetting and provide Installation Commanders with needed resources and capabilities.

Commander, Navy Installations Command Comments

The Deputy Commander, Navy Installations Command, responding for the Commander, Navy Installations Command, disagreed with the recommendation. The Deputy Commander stated CNIC already provides access control resources and capabilities to Navy installations. The Deputy Commander stated Navy installations are generally NCIC-capable, and NCACS is in the process of attaining even greater and more-facilitated NCIC access through process improvements. Furthermore, the Deputy Commander stated that the Inspector General's conclusions regarding NCIC-check capability of Navy installations were based upon interviews of persons who did not have full knowledge of the system, such as gate guards who are not responsible for credentialing.

Our Response

Comments from the Deputy Commander, Navy Installations Command, were nonresponsive. As noted in our draft report, of the 10 Navy installations visited, 7 did not have access to the NCIC database. Furthermore, during our audit, N3AT's Program Director acknowledged that not all Navy installations were performing NCIC checks prior to providing the NCACS credential to contractor employees. NCACS credentials provide contractors the ability to gain unescorted installation access. As noted in our draft report, DoD DTM 09-012 requires contractors without a Federal PIV to be vetted through the NCIC database to gain unescorted access to DoD installations. Given that the DoD DTM 09-012 established the NCIC check requirement in December 2009, the required NCIC capability should already be established at all Continental United States Navy installations. Additionally, our report findings and conclusions regarding NCIC check capabilities were based upon interviews with and documentation obtained from installation security officers, security directors, physical security specialists, access control officers, and N3 operations officers who were fully knowledgeable regarding the status of their installation physical security and access control capabilities. We request that the Commander, Navy Installations Command, reconsider the recommendation and provide additional comments on the final report.

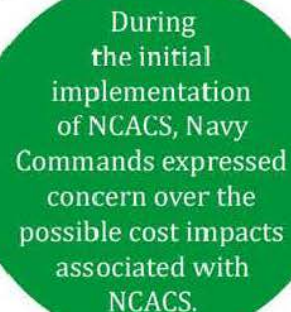
Finding B

NCACS Projected Costs Not Supported

CNIC N3AT misrepresented projected costs to operate NCACS as a no-cost, low-cost solution. This occurred because CNIC N3AT did not perform a comprehensive BCA and issued policy that prevented transparent accounting for actual NCACS costs. As a result, the Navy is unable to account for actual NCACS-related charges from contractor companies. For example, we found that the Navy has incurred NCACS-related charges of at least \$1.28 million for 17 of the 30,702 contractor companies enrolled. Additionally, other DoD Components located on Navy-controlled installations and joint bases may be inadvertently absorbing the costs of NCACS.

Costs Not Identified or Properly Represented

CNIC N3AT misrepresented the projected costs incurred by the Navy to operate NCACS. CNIC N3AT marketed NCACS to DoD and the Navy as a no-cost, low-cost access control solution. CNIC N3AT officials claimed NCACS was low-cost because fees paid by the participating contractors would serve as the primary source of revenue for the service provider, Eid Passport. According to CNIC N3AT, the costs borne by the Navy for NCACS were limited to providing phone lines, electrical power, and space for Rapidgate kiosks. However, during the initial implementation of NCACS, Navy Commands expressed concern over the possible cost impacts associated with NCACS.



During the initial implementation of NCACS, Navy Commands expressed concern over the possible cost impacts associated with NCACS.

At the request of the Shore Readiness Division (OPNAV N46), the Naval Air Systems Command (NAVAIR) and Naval Supply Systems Command (NAVSUP) conducted cost analyses and impact assessments for NCACS implementation. Both the NAVSUP memorandum, "Cost Analysis and Impact of RAPIDGate/Navy Commercial Access Control System (NCACS) Implementation," November 18, 2011, and the Naval Air Systems Command, "NAVAIR Cost Analysis and Impact of RAPIDGate/NCACS," November 21, 2011, concluded that the cost reportedly absorbed by contractors to obtain Rapidgate credentials are transferred back to the Navy in the form of higher contract overhead costs and other contract fees. Additionally, NAVSUP performed a detailed cost analysis comparing NCACS and Common Access Cards, concluding NCACS credentials could potentially cost 10 times as much as Common Access Cards over a 10-year period. Furthermore, one contractor

working on the Joint Strike Fighter program stated it planned to increase the cost of its contract approximately \$1 million annually over a 5-year period as a result of NCACS. Due to potential increased contract costs and the nature of the Joint Strike Fighter program, the program officials determined the contractor employees were eligible for issuance of Common Access Cards as authorized under DoD policy.

CNIC Cost Claims Unreliable and Unsubstantiated

CNIC N3AT's low-cost claims were unreliable because CNIC N3AT did not perform a comprehensive BCA and were unsubstantiated because they issued policy preventing transparent accounting of NCACS costs. CNIC N3AT did not perform a comprehensive BCA in response to the Shore Readiness Division (OPNAV N46) request for cost analyses and impact assessments of NCACS. In November 2011, the Program Director, CNIC N3AT, conducted an NCACS BCA that concluded CNIC would realize a cost avoidance exceeding \$295 million over 5 years by utilizing the Rapidgate system. However, CNIC N3AT's BCA did not meet the BCA requirements contained in the Department of the Navy Chief Information Officer Memorandum, "Required Use of The Department of The Navy (DON) Enterprise Information Technology Standard Business Case Analysis (BCA) Template," June 30, 2011. The Department of the Navy BCA template includes performance measures (baseline, target, and goal), operational impact, financial costs, and savings projections based on an approved methodology. However, CNIC N3AT's BCA did not include all the elements required by the Department of the Navy Memorandum. For example, CNIC N3AT did not include a financial analysis of net present value, break-even point, benefit cost ratio, and financial return on investment over the life of the program in its BCA. Furthermore, CNIC N3AT's BCA analysis did not include any non-financial benefits and risks associated with NCACS, such as interoperability, efficiency, and reliability of the system. The Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), as the resource sponsor for CNIC, should perform an independent BCA for NCACS in accordance with the Department of Navy Chief Information Officer requirements and determine the most efficient way forward.

Additionally, CNIC N3AT officials claimed that NCACS was a low-cost solution because fees paid by the participating contractors would serve as the primary source of revenue for the service provider. Despite lacking authority to direct the contract management of other Navy commands, CNIC N3AT issued policy that prevented contractors from directly charging Navy contracts for NCACS, which hindered accounting of actual program costs. CNIC issued Notice 5530, "Navy Commercial Access Control System Within Continental United States Regions, Navy Region Hawaii, and Joint Region Marianas," July 5, 2012, requesting that all contracts involving physical access to Navy installations include a

provision that costs incurred by the contractor to obtain Rapidgate credentials are not reimbursable as a direct cost to the Navy. However, CNIC Notice 5530 does not prohibit contractors from indirectly charging for Rapidgate credentials, reducing the visibility of NCACS costs. CNIC N3AT officials acknowledged that costs would be borne by the Navy component in indirect contract costs.

Furthermore, CNIC Instruction 5530.14, "CNIC Ashore Protection Program," July 7, 2011, "applies NCACS requirements to all Navy facilities and non-Navy organizations physically located on or aligned to U.S. Navy-controlled installations." DoD Components located on Navy-controlled installations and joint bases that wish to have contractors receive routine physical access without the hindrance of a daily pass are required to enroll in Rapidgate. However, these DoD Components are not subject to the provision requiring them to disallow contractors to charge for Rapidgate credentials. Therefore, other DoD Components located on Navy-controlled installations and joint bases could be directly or indirectly charged for NCACS participation. Because CNIC is not authorized to direct commercial vendor contract management for other Navy Commands and DoD Components, the Assistant Secretary of the Navy (Research, Development, and Acquisition) should review NCACS contract language concerning reimbursement of NCACS or Rapidgate credential costs and take appropriate action.

NCACS Costs are Unknown

CNIC N3AT was not able to account for, or adequately project, NCACS costs to the Navy. In its current state, the costs associated with NCACS are unknown but could be exorbitant. For example, contractors charged the Navy indirectly for costs incurred to participate in the NCACS program. We identified 17 contractors that charged the Navy over \$1.28 million for costs incurred to purchase Rapidgate credentials through overhead or other indirect charges. See Appendix B for more information on the evaluation of the 17 contractors and associated cost. According to the NAVSUP cost analysis completed in November 2011, the NCACS program had 9,657 companies and 64,924 contractor employees enrolled. NAVSUP concluded that Eid Passport as the sole NCACS service provider was potentially earning between \$12 and \$15 million annually for Rapidgate services provided to the Navy, which could be charged back to the Navy as indirect costs. According to CNIC N3AT's "NCACS In Action" report dated March 1, 2013, there were 30,702 companies enrolled with 298,204 NCACS participants. As of March 2013, NAVSUP concluded that Eid Passport



We identified 17 contractors that charged the Navy over \$1.28 million for costs incurred to purchase Rapidgate credentials through overhead or other indirect charges.

was realizing annual revenue of at least \$53 million which could be indirectly charged back to the Navy. Therefore, the Navy spent an unknown amount of funds while possibly taxing other DoD Components to pay for NCACS, a system that provides weak security as discussed in Finding A with no valid contractual coverage as discussed in Finding C. However, until the Navy receives agreement from other DoD Components and adjusts policy to adequately address those possibly affected by the implementation of NCACS, the Navy will be unable to ensure non-Navy tenant activities and Military Services located on Navy-controlled installations and joint bases do not inadvertently fund NCACS.

Recommendations, Management Comments, and Our Response

Recommendation B.1.

We recommend the Assistant Secretary of the Navy (Research, Development, and Acquisition), review the use of Navy Commercial Access Control System/Rapidgate contract language concerning contractor reimbursement and take appropriate action, if necessary.

Assistant Secretary of the Navy (Research, Development, and Acquisition) Comments

The Director, Program Analysis and Business Transformation and Director, Services Acquisition, Office of the Deputy Assistant Secretary of the Navy (Acquisition and Procurement), responding for the Assistant Secretary of the Navy (Research, Development, and Acquisition), agreed with the recommendation. The Director stated he will initiate and complete a review of the Navy Commercial Access Control System/Rapidgate contract language to ensure contract language is consistent with the Federal Acquisition Regulation (FAR) Subpart 31.2 by October 25, 2013. The Director stated he will take appropriate action based on the review.

Our Response

Comments from the Director were responsive, and no further comments are required.

Recommendation B.2.

We recommend the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics):

- a. **Obtain an independent comprehensive business case analysis for the Navy Commercial Access Control System in accordance with Department of the Navy Chief Information Officer Memorandum “Required Use of Department of the Navy (DON) Enterprise Information Technology Standard Business Case Analysis (BCA) Template,” based on an approved methodology such as the Economic Viability Tool, and**
- b. **Determine the way forward for contractor installation access based on the findings of the independent, comprehensive business case analysis.**

Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics) Comments

The Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), agreed with the recommendation. The Director stated the Commander, Navy Installations Command, has requested that the Director, Assessments Division (OPNAV N81), provide an expedited independent verification and validation of the NCACS BCA. Additionally, the Director stated OPNAV N46 will work with the Assistant Secretary of the Navy (Financial Management and Comptroller), OPNAV N81, CNIC, and other Navy stakeholders to review, validate, and adjust format/template accordingly to ensure the completed BCA fully complies with the DoD Inspector General’s requirements.

The Director stated if follow-on actions are required as determined by the BCA, then OPNAV N46 will work with CNIC to ensure development of consistent policies and procedures across all Navy regions for contractor installation access control. The Director stated, at a minimum, the policies and procedures will provide reciprocity for contractors with existing federally sponsored background investigations. Finally, the Director stated CNIC, with OPNAV N46 oversight, will also work with Echelon II commands to create a visitor control process that complies with DoD and Department of the Navy installation security standards.

Our Response

Comments from the Director were responsive, and no further comments are required.

Finding C

CNIC Circumvented Competitive Contracting Requirements

The CNIC N3AT Program Director, N3AT Assistant Program Managers for physical security, and the Naval District Washington Chief Information Officer, circumvented competitive contracting requirements, using two different contracting offices and inappropriate contracting methods to implement and execute NCACS. Specifically, CNIC N3AT:

- directed a prime contractor, in October 2011, and September 2012, to enter into unauthorized commitments for out-of-scope work;
- restricted full and open competition; and
- allowed Eid Passport to continue providing services since November 1, 2012, without a contract.

This occurred because CNIC N3AT did not have contracting authority and developed a COC as an administrative approach to maintain a relationship with Eid Passport. As a result, the Navy expended \$1,179,299 in disallowable costs for Eid Passport's services and equipment. Furthermore, CNIC N3AT lacked oversight of, and legal recourse against, Eid Passport should Eid Passport fail to meet the requirements for implementing the Navy's identity management and perimeter installation access control solution.

Contractor Competition is Required

The Competition in Contracting Act of 1984 requires agencies to obtain full and open competition using competitive procedures in their procurement activities, unless otherwise authorized by law. Contracts awarded using full and open competition permit all prospective contractors that meet certain criteria to submit proposals. Agencies are generally required to perform acquisition planning and conduct market research to promote and provide for full and open competition.

Rapidgate Procurement History

According to the "Navy Marine Corps Acquisition Regulation Supplement (NMCARS)," January 2013, CNIC does not have contracting authority and is required to obtain contractual coverage from the appropriate Head of Contracting Activity depending on the type of procurement. Due to CNIC's lack of contracting authority, a Government

Purchase Card (GPC) is the only contractual vehicle available to CNIC that does not require formal procurement support.

In April 2010, CNIC N3AT purchased seven, 1-year Rapidgate system subscriptions totaling \$2,499.49, using a CNIC GPC, with NAVSUP-delegated contracting authority, from the General Services Administration schedule. According to the NAVSUP Instruction 4200.99, "Department of the Navy (DON) Policies and Procedures for the Operation and Management of the Government-Wide Commercial Purchase Card Program (GCPC)," October 13, 2006, the GPC shall be used to make open market purchases for supplies and services not to exceed \$2,500. The General Services Administration purchase order forms indicated that the price for seven Rapidgate subscriptions was \$3,059.00. However, CNIC requested and was granted a price change authorization which resulted in a final price of \$2,499.49, \$0.51 below the micro-purchase threshold. In April 2011, CNIC N3AT renewed the seven Rapidgate system subscriptions totaling \$2,499.49 for an additional year using the same GPC methodology on another individual's GPC. However, the April 2011 purchase order was canceled in October 2011 due to objections from NAVSUP regarding the contractual manner in which Rapidgate services were acquired.

Prime Contractor Directed to Enter Into Unauthorized Commitments

Without contracting authority, CNIC N3AT officials, with assistance from the Naval District Washington Chief Information Officer, directed a prime contractor, 3e Technologies International (3eTI), to enter into unauthorized commitments totaling \$1,179,299 without obtaining approval from the contracting officers. According to the Federal Acquisition Regulation (FAR) 43.102(a)(3), only contracting officers can direct or encourage the contractor to perform work. However, CNIC officials directed 3eTI personnel to subcontract for Eid Passport services and equipment on two unrelated contracts awarded by Naval Sea Systems Command contracting offices.



CNIC N3AT officials...directed a prime contractor, 3e Technologies International, to enter into unauthorized commitments totaling \$1,179,299 without obtaining prior approval from the contracting officers.

In October 2011, 3eTI subcontracted with Eid Passport to purchase eight Rapidgate system subscriptions valued at [REDACTED] under a contract awarded by Naval Surface Warfare Center (NSWC) Panama City.⁶ The accompanying Statement of Work between

⁶ Contract No. N61331-08-D-0043 Delivery Order 0006 was awarded by NSWC Panama City on April 13, 2011.

3eTI and Eid Passport provides for the installation of Rapidgate at all Navy installations in the Continental United States, Hawaii, and Marianas. However, 3eTI's contract with NSWC Panama City for the Navy-Wide Virtual Perimeter Monitoring System was restricted to the development and demonstration of an interface capability at installations in Naval District Washington. The contract did not include provisions for installation and maintenance of Rapidgate at all Navy installations in the Continental United States, Hawaii, and Joint Region Marianas. Additionally, NSWC Panama City contracting personnel stated they were unaware of the 3eTI subcontract with Eid Passport. Therefore, 3eTI's subcontract with Eid Passport was an unauthorized commitment for out-of-scope work that would normally require use of competitive contracting procedures. The Chief of Contracting at NSWC Panama City should review the 3eTI subcontract and determine whether the costs should be disallowed and recouped in accordance with FAR 42.8, "Disallowance of Costs," or if ratification actions may be appropriate in accordance with FAR 1.602-3, "Ratification of Unauthorized Commitments." After the review is completed, the Chief of Contracting should take the appropriate contracting actions.

Furthermore, on September 27, 2012, 3eTI subcontracted with Eid Passport to purchase Rapidgate proprietary handheld scanners, valued at [REDACTED] on a contract awarded by NSWC Port Hueneme.⁷ This subcontract was initiated by the Naval District Washington Chief Information Officer at the direction and request of CNIC N3AT officials without working through the procuring contracting officer. However, 3eTI's contract awarded by NSWC Port Hueneme was for the design, development, integration test, and implementation of the Critical Infrastructure Sensor Network and it did not include provisions for the purchase of handheld scanners. Additionally, the NSWC Port Hueneme contracting officer was unaware of the subcontract and stated 3eTI did not have an approved purchasing system in accordance with FAR 44.201-1(b). FAR Part 44.201 prohibits any subcontracting by a contractor without an approved purchasing system if subcontracting amount exceeds 5 percent of the contract value. Since the estimated contract value was \$9,923,241, the value for 3eTI's subcontract with Eid Passport was more than 10 percent of the estimated contract value and therefore should have required prior approval from the contracting officer. Therefore, 3eTI's subcontract with Eid Passport was an unauthorized commitment for out-of-scope work that would require use of competitive contracting procedures or a Justification and Approval for sole source. The Chief of Contracting at NSWC Port Hueneme should review the 3eTI subcontract and determine whether the costs should be disallowed and recouped in accordance with FAR 42.8, "Disallowance of Costs," or if ratification actions may be appropriate in accordance with FAR 1.602-3, "Ratification of Unauthorized Commitments." After the

⁷ Contract No. N63394-12-C-5127 was awarded by NSWC Port Hueneme on September 14, 2012.

review is completed, the Chief of Contracting should take the appropriate contracting actions. Furthermore, the Assistant Secretary of the Navy (Research, Development, and Acquisition), in conjunction with the Director of Contracts, Naval Sea Systems Command, should conduct an accountability review relating to the unauthorized commitments including full access to all information and individuals necessary to conduct the review.

CNIC Officials' Actions Restricted Full and Open Competition

After entering into unauthorized commitments with Eid Passport, in June 2012, CNIC N3AT issued an NCACS sources sought notice for market research to determine which vendors had the capabilities to meet NCACS requirements. According to the NCACS sources sought notice, the purpose was to obtain information regarding the availability and capability of all qualified sources interested in participating as a NCACS commercial credentialing service. However, according to the NCACS sources sought notice, no contract would be issued, and contract proposals were not being accepted. CNIC N3AT officials stated there were two responses to the sources sought notice, one from Eid Passport and another from Intellicheck Mobilisa. Despite previous statements of work noting that Eid Passport vetted individuals against unreliable databases, CNIC N3AT determined only Eid Passport's response qualified them to and selected them to continue to provide services for NCACS. However, instead of beginning appropriate contracting procedures to maintain the services provided by Eid Passport, CNIC N3AT officials issued a COC, which is not a contract, to Eid Passport based on its response to the sources sought notice.

Navy Lacks Contractual Coverage for Eid Passport Services

While CNIC N3AT has been receiving services from Eid Passport to implement Rapidgate at all Navy installations and facilities in the Continental United States, Hawaii, and the Marianas Islands since April 2010, the Navy has not had valid contractual coverage since November 1, 2011. Instead of providing for full and open competition, CNIC N3AT officials directed a prime contractor to enter into unauthorized commitments for Eid Passports' proprietary Rapidgate system and then issued a COC in October 2012 to allow Eid Passport to continue providing services for the NCACS program. The COC explicitly stated it is not a Federal contract and does not constitute an enforceable agreement. Furthermore, the COC did not meet the definition of a contract as stated in FAR Part 2.101 because a warranted contracting officer did not sign it and it did not bind the Federal Government

for any obligation of funds. As of May 2013, CNIC N3AT has allowed Eid Passport to continue providing Rapidgate to support NCACS without contractual coverage.

Appropriate Contracting Authority Was Not Used



CNIC N3AT officials improperly directed a prime contractor to enter into unauthorized commitments.

CNIC N3AT officials improperly directed a prime contractor to enter into unauthorized commitments, used inappropriate contracting methods, and incorrectly developed the COC because they did not have contracting authority. The “Navy Marine Corps Acquisition Regulation Supplement (NMCARS),” January 2013, establishes uniform Department of the Navy policies and procedures for implementing and supplementing the FAR and the Defense Federal Acquisition Regulation Supplement. NMCARS identifies 11 Head of Contracting Activities (HCAs) in the Navy responsible for managing and overseeing their respective contracting missions. According to the NMCARS, CNIC does not have HCA authority and is therefore required to obtain contractual coverage from the proper HCA depending on the type of procurement. CNIC N3AT officials justified their use of the COC relationship with Eid Passport stating their requests for contractual coverage from an appropriate HCA were cumbersome and difficult. For example, after cancellation of the GPC procurement of Rapidgate, CNIC N3AT approached an HCA, Naval Facilities Engineering Command, to place NCACS into a contract administered by Naval Facilities Engineering Command. However, Naval Facilities Engineering Command declined to support the request resulting in CNIC N3AT officials inappropriately directing an NSWC Panama City prime contractor to subcontract for Rapidgate. After reviewing the NSWC Panama City subcontract, CNIC general counsel was concerned and notified CNIC N3AT officials that this type of contract would not receive any legal support in the future. Subsequently, CNIC N3AT officials developed the COC as an administrative approach to maintain a relationship with Eid Passport that did not require an acquisition vehicle. According to CNIC N3AT officials, the COC leverages the Navy’s stance as a third-party beneficiary⁸ of the implied contract(s) between NCACS participants and Eid Passport. However, the Navy continued to receive services, such as identity vetting, credential creation, and database maintenance, directly from Eid Passport for maintenance and management of the NCACS program. The Assistant Secretary of the Navy (Research, Development, and Acquisition) should initiate a review of the inappropriate contracting practices related to NCACS and Eid Passport and establish a corrective action plan to resolve the contracting improprieties.

⁸ A third-party beneficiary is a party who stands to benefit from the execution of the contract even though that was not the intent of either contracting party.

Navy Spent Over \$1.1 Million in Potentially Unallowable Costs and Lacked Oversight and Legal Recourse Against Eid Passport

The Navy expended \$1,179,299 in potentially unallowable costs for Eid Passport's services and equipment. Furthermore, CNIC N3AT lacked oversight of, and legal recourse against, Eid Passport in the event the service provider failed to meet its responsibilities. The COC did not bind Eid Passport to perform the actions outlined in the COC and did not provide CNIC N3AT the ability to legally enforce the stated requirements because the COC did not constitute an enforceable agreement. For example, the COC required Eid Passport to comply with DoD Information Assurance Certification and Accreditation Process, and the NCACS Standard Operating Procedures. Additionally, under the COC, Eid Passport will be subjected to an annual compliance audit by CNIC N3AT. However, without a contract or legally binding agreement, CNIC N3AT officials did not have any legal options to enforce compliance with the stated requirements. The only viable administrative option available to CNIC N3AT is to terminate the COC issued to Eid Passport. However, this would render NCACS inoperable because Eid Passport maintains the NCACS program data and the database used for authentication.

Conclusion

The Navy Commercial Access Control System, using Rapidgate, did not effectively mitigate access control risks, and did so at a potentially exorbitant price to the Navy. Although NCACS did not comply with Federal and DoD vetting standards and did not effectively mitigate access control risks, CNIC N3AT took extraordinary measures to ensure the program continued to operate without contracting authority. CNIC N3AT personnel used inappropriate contracting practices, such as directing a prime contractor to enter into unauthorized commitments to maintain Eid Passport's Rapidgate system and issuing policy that prevented the Navy from fully accounting for NCACS costs. These actions appear to have provided Eid Passport with a competitive advantage, allowing them to realize substantial revenue annually for providing credentialing and vetting services for the Navy without a contract. See Finding A for information on access control risks and Finding B for the costs associated with NCACS. Due to the improprieties of NCACS and consistent violations of Federal acquisition requirements, the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), should review CNIC N3AT officials' actions, and determine whether administrative actions should be taken, if appropriate.

Recommendations, Management Comments, and Our Response

Recommendation C.1.

We recommend the Assistant Secretary of the Navy (Research, Development, and Acquisition), initiate a review of the inappropriate contracting practices related to the Navy Commercial Access Control System and establish a corrective action plan to resolve the contracting improprieties.

Assistant Secretary of the Navy (Research, Development, and Acquisition) Comments

The Director, Program Analysis and Business Transformation and Director, Services Acquisition, Office of the Deputy Assistant Secretary of the Navy (Acquisition and Procurement), responding for the Assistant Secretary of the Navy (Research, Development, and Acquisition), agreed with the recommendation. The Director stated the Office of the Deputy Assistant Secretary of the Navy (Acquisition and Procurement), will initiate and complete a review of the contracting practices and establish a corrective action plan if it is determined that there were any improprieties. The Office of the Deputy Assistant Secretary of the Navy (Acquisition and Procurement), expects to finish their review of the contracting practices by October 25, 2013.

Our Response

Comments from the Director were responsive, and no further comments are required.

Recommendation C.2.

We recommend the Assistant Secretary of the Navy (Research, Development, and Acquisition), in conjunction with the Director of Contracts, Naval Sea Systems Command, initiate an accountability review relating to the unauthorized commitments including full access to all information and individuals necessary to conduct the review.

Assistant Secretary of the Navy (Research, Development, and Acquisition) and Director of Contracts, Naval Sea Systems Command Comments

The Director, Program Analysis and Business Transformation and Director, Services Acquisition, Office of the Deputy Assistant Secretary of the Navy (Acquisition and Procurement), responding for the Assistant Secretary of the Navy (Research, Development,

and Acquisition), and the Associate Director of Contracts, Naval Sea Systems Command, responding for the Director of Contracts, Naval Sea Systems Command, agreed with the recommendation. The Director, Program Analysis and Business Transformation and Director, Services Acquisition, Office of the Deputy Assistant Secretary of the Navy (Acquisition and Procurement), and the Associate Director of Contracts, Naval Sea Systems Command, stated they will perform the recommended accountability review by October 25, 2013.

Our Response

Comments from the Director, Program Analysis and Business Transformation and Director, Services Acquisition, Office of the Deputy Assistant Secretary of the Navy (Acquisition and Procurement), and the Associate Director of Contracts, Naval Sea Systems Command, were responsive, and no further comments are required.

Recommendation C.3.

We recommend the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), perform a review of the Commander, Naval Installations Command Antiterrorism officials and consider administrative actions, if appropriate for:

- a. Implementing the Navy Commercial Access Control System using Eid Passport's Rapidgate system that allows contractors to have access to Navy installations without having their identities vetted through mandatory authoritative databases.**
- b. Implementing the Navy Commercial Access Control System without a comprehensive business case analysis.**
- c. Improperly directing a prime contractor to enter into unauthorized commitments of Navy funds.**

Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics) Comments

The Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), partially agreed with the recommendation. The Director stated that any review of CNIC employees, including the determination as to whether a review is required, is the responsibility of the Commander, Navy Installations Command. The Director stated the Commander, Navy Installations Command, will take administrative action as appropriate pending the findings of reviews conducted pursuant to recommendations B.2, C.1, C.2, and C.4, as well as OPNAV N81 independent review of the BCA.

Our Response

Comments from the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), were partially responsive. We agree that reviews should be conducted pursuant to recommendations B.2, C.1, C.2, and C.4, and if there are findings, administrative action be considered. However, we believe the review of CNIC employee actions regarding NCACS implementation and contracting should be performed by an entity independent of the Commander, Navy Installations Command. An independent entity would not have a vested interest in the NCACS program and would be free of potential conflicts in assessing the CNIC employee actions. We request the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), reconsider the recommendation and provide additional comments in response to the final report.

Recommendation C.4.

We recommend the Chief of Contracting offices at Naval Surface Warfare Centers Port Hueneme and Panama City:

- a. Review the 3e Technologies International subcontract and determine whether the costs should be disallowed and recouped in accordance with Federal Acquisition Regulation 42.8, "Disallowance of Costs," or if ratification actions may be appropriate in accordance with Federal Acquisition Regulation 1.602-3, "Ratification of Unauthorized Commitments," and**
- b. Take the appropriate contracting actions in accordance with the determinations of the review.**

Chief of Contracting Offices, Naval Surface Warfare Centers Port Hueneme and Panama City Comments

The Associate Director of Contracts, Naval Sea Systems Command, responding for the Chief of Contracting offices at Naval Surface Warfare Centers Port Hueneme and Panama City, agreed with the recommendation. The Associate Director stated Naval Sea Systems Command will conduct the review of the two contract actions specified in the report by October 25, 2013.

Our Response

Comments from the Associate Director were responsive, and no further comments are required.

Appendix A

Scope and Methodology

We conducted this performance audit from October 2012 through June 2013 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 performed the audit to determine whether NCACS is mitigating access control risks to Navy installations. NCACS was implemented at all 61 Navy installations within the Continental United States. Of the 61 Navy installations, we non-statistically selected a sample of 10 installations to determine whether NCACS identity vetting complies with Federal and DoD requirements. The locations selected represent at least one installation from each of the six Navy regions within the Continental United States. According to CNIC N3AT management, NCACS implementation requirements did not vary by regions or installations. Therefore, the findings in this report may apply to all Navy installations in the Continental United States.

We interviewed personnel, performed walkthroughs of Navy installation Pass and Identification offices and access control points, obtained and reviewed 104 NCACS waiver requests, obtained and reviewed 47 contracts and other funding documentation for companies enrolled in NCACS, and reviewed supporting documentation for identity vetting at 10 Navy installations. From the interviews conducted with contracting officers and contracting officer representatives from five of the six Navy Regions, we identified 17 contractors that charged the Navy for costs incurred to purchase Rapidgate credentials. We reviewed contractor Requests for Equitable Adjustments, overhead prices, and other indirect costs. The records and actions reviewed occurred from April 2010 through May 2013. See Appendix B for a listing of the 17 contractors and the related NCACS charges.

~~(FOUO)~~ Our review included the following Navy installations.

- Naval District Washington:

- [REDACTED]
- [REDACTED]

- ~~(FOUO)~~ Navy Region Mid-Atlantic:
 - [REDACTED]
 - [REDACTED]
- Navy Region Southeast:
 - [REDACTED]
 - [REDACTED]
- Navy Region Midwest:
 - [REDACTED]
- Navy Region South West:
 - [REDACTED]
 - [REDACTED]
- Navy Region Northwest:
 - [REDACTED]

Use of Computer-Processed Data

We obtained and used computer-processed data. Specifically, we used paper copies of the public record check results from SecurTest, Inc., and General Information Services, Inc., databases to determine the accuracy and reliability of the information reported. We compared the results of initial public record checks against the results of the periodic and renewal checks and discussed the inaccuracies of the publicly accessible databases in Finding A. We did not evaluate the databases used to perform the public record checks because Eid Passport acknowledged the public data sources used to conduct record checks were not always up-to-date, complete, accurate, or available.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO), the Department of Defense Inspector General (DoD IG), and the Naval Audit Service issued six reports discussing DoD's implementation of Homeland Security Presidential Directive 12, physical access control, and force protection. Unrestricted GAO reports can be accessed over the Internet at <http://www.gao.gov>. Unrestricted DoD IG reports can be accessed at

<http://www.dodig.mil/pubs/index.cfm>. Naval Audit Service reports are not available over the Internet.

GAO

GAO Report No. GAO-11-751, "Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards," September 2011

GAO Report No. GAO-08-292, "Electronic Government: Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards," February 2008

DoD IG

DoDIG Report No. DODIG-2012-122, "DoD Should Procure Compliant Physical Access Control Systems to Reduce the Risk of Unauthorized Access," August 29, 2012 (Document is FOUO)

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

DoDIG Report No. D-2008-104, "DoD Implementation of Homeland Security Presidential Directive-12," June 23, 2008

Navy

Naval Audit Service Report No. N2011-0033, "Contracts Awarded to Selected Contractors by Naval Supply Systems Command and Naval Facilities Engineering Command Contracting Activities," May 5, 2011 (Document is FOUO)

Appendix B

Identified Contractor Companies and Amounts Charged for NCACS-Related Costs

Contractor Company	Amount Charged	Documentation Provided
ASG Solutions Corporation	\$743	Request for Equitable Adjustment (REA) to contract N00178-05-D-4191-JM01
WalBridge Aldinger Company	27,497	REA to contract N69450-09-C-0758
The Ross Group Construction Corp.	30,878	REA to contract N69450-10-D-0771-0002
W.G. Yates & Sons Construction Co.	77,436	REA to contract N62467-05-D-0183
J.J. Sosa & Associates, Inc.	5,390	REA to contract N69450-10-D-0783-0001
Akea, Inc	4,771	REA to contract N69450-09-C-1294
Orion Marine Construction	10,742	REA to contract N69450-09-C-1259
Del-Jen, Inc.	49,817	REA to contract N69450-07-D-0770
Gottfried Construction LLC	21,666	REA to contract N62467-06-D-3140-0006
Power Services, Inc.	1,193	REA to contract N69450-10-C-7328
W.F. Magann	5,693	REA to contract N40085-11-C-0200
	9,878	REA to contract N40085-09-C-5058
McLean Contracting Co.	18,673	REA to contract N40085-11-C-0001
ACEPEX Management Corp	10,017	REA to contract N40085-06-D-1260
Goodwill Industries	199,148	Overhead charge to contract N00189-09-C-Z003
DynCorp international	99,197	Overhead documentation provided
BAE Systems	235,640	Overhead documentation provided
	202,870	Overhead documentation provided
Huntington Ingalls	270,180	Overhead documentation provided
Total	\$1,281,429	

Glossary

Background Check: The act of reviewing both confidential and public information to investigate a person's history. Background checks are commonly performed by employers to ensure that: (1) an employee is who he or she says they are, (2) to determine that the individual does not have a damaging history (such as criminal activity) that may reflect poorly on the company, (3) to confirm information that an applicant included on their application for employment.

Contractor Employee: An individual who performs work for or on behalf of any agency under a contract and who, in order to perform the work specified under the contract, will require access to space, information, information technology systems, staff, or other assets of the Federal Government. Such contracts include, but are not limited to:

- personal services contracts,
- contracts between any non-Federal entity and any agency, and
- subcontracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the agency.

Installations: Real DoD properties including bases, stations, forts (including National Guard and Federal Reserve Centers), depots, arsenals, plants (both contractor- and Government-operated), hospitals, terminals, and other special mission facilities, as well as those used primarily for military purposes.

National Agency Check With Written Inquiries: Consists of searches of the Office of Personnel Management Security Suitability Investigations Index; the Defense Clearance and Investigations Index; Federal Bureau of Investigation Identification Division fingerprint name file and fingerprint chart; Federal Bureau of Investigation Records Management Division files; written inquiries; and record searches covering specific areas of a subject's background during the past 5 years.

PIV Credential: A physical artifact (for example, an identity card or a "smart" card) issued to an individual that contains stored identity credentials (such as a photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable).

Public Record Check: The act of reviewing any publicly available information, minutes, files, accounts or other records (including hearsay in the record) that may not be up-to-date, complete, accurate, or available to investigate a person's history to determine if the individual has a damaging history (such as criminal activity).

Rapidgate System 1-Year Subscription: As listed in Eid Passport's General Services Administration General Schedule GS-35F-0436U, the 1-year Rapidgate services include registration; employee background screenings; identification badges; access control authentication; reporting; equipment maintenance; and training. Rapidgate equipment and software include: registration station(s), guard station(s), handheld reader device(s), antenna equipment, and identification badges. Eid Passport retains all rights and title to Rapidgate equipment, software, and data. Eid Passport charges enrollment and registration fees to vendors. Minimum ordering activity qualifications: the total number of vendor companies divided by the total number of access control points must be at least 50 at each facility/installation.

Vetting: An evaluation of an applicant's or a cardholder's character and conduct for approval, acceptance, or denial for the issuance of an access control credential or physical access.

Management Comments

Department of the Navy Comments



THE DEPUTY UNDER SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

04 AUG 2013

MEMORANDUM FOR THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Department of the Navy's Response to Department of Defense Inspector
General Report Project Number D2013-D000LC-0008.000 dated 24 Jun
13

The Department of the Navy (DON) appreciates the opportunity to respond and comment on the Department of Defense Inspector General Report Project Number D2013-D000LC-0008.000 dated 24 Jun 13.

The DON concurs with most of the recommendations and has established target dates to address those recommendations. The Commander, Navy Installations Command non-concurs with recommendations A.1.-A.3 in the report. The Director, Shore Readiness Division, Deputy Chief of Naval Operations (Fleet Readiness and Logistics) non-concurs with recommendation C.3. CNIC requests to further discuss these four findings. Details of our specific comments and recommendations are attached.

[REDACTED]


Robert Martinage
ACTING

Attachment:
As stated

Department of the Navy Comments (cont'd)

**DEPARTMENT OF DEFENSE INSPECTOR GENERAL REPORT
PROJECT NO. D2013-D000LC-0008.000 DATED 24 JUNE 2013**

**“NAVY COMMERCIAL ACCESS CONTROL SYSTEM DID NOT
EFFECTIVELY MITIGATE ACCESS CONTROL RISKS”**

The Navy's responses to the Department of Defense Inspector General's (DODIG) recommendations are as follows:

RECOMMENDATION A.1.: The DODIG recommended that the Commander, Navy Installations Command, immediately discontinue the use of Rapidgate and any other system that exclusively uses publicly available databases to vet and adjudicate contractor employees accessing Navy installations, and replace it with a system or process that meets Federal and DoD requirements for background vetting.

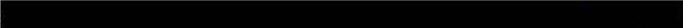
RESPONSE (CNIC): Non-concur. Navy Commercial Access Control System (NCACS) standards meet or exceed Federal and DoD requirements for background vetting. The current Commercial Credential Source (CCS) is a federally approved Personal Identity Verification – Interoperable (PIV-I) compliant company. In addition to the commercial vetting conducted by the NCACS provider, the Navy currently conducts the National Crime Information Center (NCIC) check and final issuance of the credential. CNIC will always maintain oversight and quality control of the final product and determines whether or not the credential is ultimately issued. Prior to acceptance into NCACS as a CCS, a credentialing firm or entity must demonstrate full compliance and capabilities in conformity with a long list of stringent requirements starting with HSPD-12, DTM 09-012, FIPS 201, DoD 5200.08-R, and more than a dozen other Federal, DoD and Navy standards/instructions. Finally, more than 36,700 companies with over 438,000 of their employees or vendors have been vetted and credentialed via NCACS. Discontinuing a successful system that has facilitated over 14,000,000 safe and secure visits will ensure there are unnecessarily long waiting lines at gates and access points at many of the Navy's installations, including some of our largest bases in [REDACTED]. The result is loss in productivity for those contractors and vendors doing business on Navy installations. Abandoning the current NCACS business solution would require the hiring of significant numbers of additional civil servants to work in base pass offices across the CNIC enterprise. This would not be feasible in a time of austerity that has occasioned not only furloughs and hiring freezes, but actual Reductions in Force (RIF) at CNIC.

Department of the Navy Comments (cont'd)

RECOMMENDATION A.2.: The DODIG recommended that the Commander, Navy Installations Command, revise Instruction 5530.14, "CNIC Ashore Protection Program," July 7, 2011, and Notice 5530, "Navy Commercial Access Control System Within Continental United States Regions, Navy Region Hawaii, and Joint Region Marianas," July 5, 2012, to require contractor employees requiring routine physical access to Navy installations for greater than six months receive the DoD Personal Identity Verification credential with the National Agency Check with Written Inquiries.

RESPONSE (CNIC): Non-concur. CNIC is in line with DoD authorities and Congressional guidance to leverage security by partnering with commercial entities, adopting commercial off-the-shelf solutions, and accepting identity credentials from Non-Federal Issuers (NFI). CNIC NCACS standards either meet or exceed the requirements mandated by DoD or cited by the DODIG. Additionally, those vendors or contractors that meet the federal standards to be issued a Common Access Card (CAC) are indeed issued a CAC. It is CNIC's understanding of current policy there are two components to issuing a CAC – physical access to an installation for greater than six months AND logical access to the Navy's networks. Many vendors or contractors meet the physical access requirement for an installation but not the access to the Navy's network, thus necessitating other alternatives for issuing credentials. Finally, the NCACS CCS vetting combined with the CNIC NCIC check encompasses those checks conducted via a National Agency Check with Written Inquiries (NACI).

RECOMMENDATION A.3.: The DODIG recommended that the Commander, Navy Installations Command;

a. Provide 

resources and capabilities needed to access National Crime Information Center and the Terrorist Screening Database.

b. Establish a process to identify which installations need resources and capabilities to access National Crime Information Center and the Terrorist Screening Database for contractor background vetting and provide Installation Commanders with needed resources and capabilities.

Department of the Navy Comments (cont'd)

RESPONSE (CNIC): Non-concur. CNIC has already accomplished the goal of providing access control resources and capabilities to Navy Installations: NCACS is the resource and is a force multiplier to Navy access control programs. Navy installations are generally NCIC-capable and NCACS is in the process of attaining even greater and more facilitated NCIC access via process improvements. DODIG's conclusions regarding NCIC-check capability of Navy installations were based upon interviews of personnel who did not have full knowledge of the system, such as gate guards who are not responsible for credentialing. Furthermore, to the extent providing resources equates to hiring additional personnel, this is not economically feasible given the fiscal constraints on the Command and is not consistent with DOD and Congressional policy that encourages adopting commercial-off-the-shelf security solutions for base access. Additionally, USD(AT&L) and the Defense Manpower Data Center are currently working access to the Terrorist Screening Database on behalf of all Department of Defense installations via the Identity Management Enterprise Services Architecture. CNIC will take advantage of this capability once it is available.

RECOMMENDATION B.1.: The DODIG recommended that the Assistant Secretary of the Navy (Research, Development and Acquisition) review the use of Navy Commercial Access Control System/Rapidgate contract language concerning contractor reimbursement and take appropriate action, if necessary.

RESPONSE (DASN(AP)): Concur. By 25 Oct 13, the Deputy Assistant Secretary of the Navy for Acquisition and Procurement (DASN(AP)) will initiate and complete a review of the Navy Commercial Access Control System/Rapidgate contract language to ensure the contract language is consistent with the cost principles and procedures in Federal Acquisition (FAR) Subpart 31.2. Based on the review, if it is determined that the contract language is inconsistent with the FAR requirements, DASN(AP) will take appropriate action.

RECOMMENDATION B.2.: The DODIG recommended that the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics):

- a. Obtain an independent comprehensive business case analysis for the Navy Commercial Access Control System in accordance with Department of Navy Chief Information Officer Memorandum "Required Use of Department of the Navy (DON) Enterprise Information Technology Standard Business Case Analysis (BCA) Template,"

Department of the Navy Comments (cont'd)

based on an approved methodology such as the Economic Viability Tool, and

b. Determine the way forward for contractor installation access based on the findings of the independent comprehensive business case analysis.

RESPONSE (N46): Concur. Commander, Navy Installations Command has requested that the Director, Assessments Division (OPNAV N81) provide an expedited independent verification and validation of the Navy Commercial Access Control System (NCACS) BCA. The BCA submitted is in full compliance with the "Required Use of the Department of the Navy (DON) Enterprise Information Technology Standard Business Case Analysis (BCA) Template, 30 Jun 11." OPNAV N46 will work with Assistant Department of the Navy Financial Management and Comptroller (FM &C), N81, CNIC and other Navy stakeholders to review, validate and adjust format/template accordingly to ensure the completed BCA meets full compliance of the DOD IG's requirements. If it's determined what, if any, follow-on actions are required then, estimated completion date for the BCA and follow-on N46 analysis and recommendations is 30 Sept 13. If determined by the BCA, OPNAV N46 will work with CNIC to ensure development of clear, concise and consistent policies and procedures across all Navy regions for contractor installation access control. At a minimum, the policies and procedures will provide reciprocity for contractors with existing federally sponsored background investigations. CNIC, with OPNAV N46 oversight, will also work with Echelon II commands to create a visitor control process that complies with DoD and DON installation security standards.

RECOMMENDATION C.1.: The DODIG recommended that the Assistant Secretary of the Navy (Research, Development and Acquisition), initiate a review of the inappropriate contracting practices related to the Navy Commercial Access Control System and establish a corrective action plan to resolve the contracting improprieties.

RESPONSE (DASN(AP)): Concur. DASN(AP) will initiate and complete a review of the contracting practices and establish a corrective action plan if it is determined that there were any improprieties. Target period for completion of the review and corrective action plan, if necessary, is 25 Oct 13. It should be noted that CNIC is working with its designated contracting agency, NAVSUP, to issue a competitive contract for the Navy

Department of the Navy Comments (cont'd)

Commercial Access Control System. Contract award is expected in Q4 FY14.

RECOMMENDATION C.2.: The DODIG recommended that the Assistant Secretary of the Navy (Research, Development and Acquisition), in conjunction with the Director of Contracts, Naval Sea Systems Command, initiate an accountability review relating to the unauthorized commitments including full access to all information and individuals necessary to conduct the review.

RESPONSE (NAVSEA/DASN(AP)): Concur. NAVSEA 02 in conjunction with DASN(AP) will perform the recommended accountability review by 25 Oct 13.

RECOMMENDATION C.3.: The DODIG recommended that the Director, Shore Readiness, Deputy Chief of Naval Operations (Fleet Readiness and Logistics), perform a review of the Commander, Navy Installations Command Antiterrorism officials and consider administrative actions, if appropriate for:

- a. Implementing the Navy Commercial Access Control System using Eid Passport's Rapidgate system that allows contractors to have access to Navy installations without having their identities vetted through mandatory authoritative databases.
- b. Implementing the Navy Commercial Access Control System without a comprehensive business case analysis.
- c. Improperly directing a prime contractor to enter into unauthorized commitments of Navy funds.

Response (N46): Partially concur. Any performance review of CNIC employees, including the determination as to whether a review is required, is the responsibility of the Commander, Navy Installations Command. Pending findings from reviews conducted by ASN(RDA)/NAVSEA based on DoD IG recommendations B.2, C.1, C.2 and C.4 as well as OPNAV N81 independent review of the BCA (recommendation B.2), Commander, Navy Installations Command will take administrative actions as appropriate. Target for completion of the review and recommended administrative actions, if necessary, is 24 Jan 14 (approximately 90 days after receipt of ASN(RDA), NAVSEA and OPNAV N81 findings). As noted previously in our response to A.1, CNIC has concluded the

Department of the Navy Comments (cont'd)

Rapidgate system allows contractors to have access to Navy installations by properly vetting their identities through the mandatory authoritative databases."

RECOMMENDATION C.4.: The DODIG recommended that the Chief of Contracting offices at Naval Surface Warfare Center Port Hueneme and Panama City:

a. Review the 3e Technologies International subcontract and determine whether the costs should be disallowed and recouped in accordance with Federal Acquisition Regulation 42.8, "Disallowance of Costs," or if ratification actions may be appropriate in accordance with Federal acquisition Regulation 1.602-3, "Ratification of Unauthorized Commitments, and

b. Take the appropriate contracting actions in accordance with the determinations of the review.

Response (NAVSEA): Concur. The review will be conducted by 25 Oct 13 and will apply to the two contract actions specified in the report, which occurred within the NAVSEA Enterprise.

Acronyms and Abbreviations

3eTI	3e Technologies International
BCA	Business Case Analysis
CNIC	Commander, Navy Installations Command
COC	Certification of Compliance
DTM	Directive Type Memorandum
FAR	Federal Acquisition Regulation
GPC	Government Purchase Card
HCA	Head of Contracting Activity
N3AT	Antiterrorism Office
NAVSUP	Naval Supply Systems Command
NCACS	Navy Commercial Access Control System
NCIC	National Crime Information Center
NSWC	Naval Surface Warfare Center
PIV	Personal Identity Verification



Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD IG Director for Whistleblowing & Transparency. For more information on your rights and remedies against retaliation, go to the Whistleblower webpage at www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison

Congressional@dodig.mil; 703.604.8324

DoD Hotline

800.424.9098

Media Contact

Public.Affairs@dodig.mil; 703.604.8324

Monthly Update

dodigconnect-request@listserve.com

Reports Mailing List

dodig_report-request@listserve.com

Twitter

twitter.com/DoD_IG

~~FOR OFFICIAL USE ONLY~~



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

~~FOR OFFICIAL USE ONLY~~