

FOR OFFICIAL USE ONLY

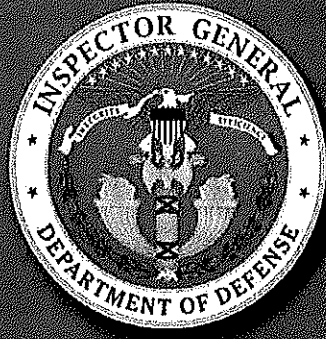
Report No. DODIG-2013-072

April 24, 2013

Inspector General

United States

Department of Defense



Data Loss Prevention Strategy Needed for the Case Adjudication Tracking System

~~This document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.~~

FOR OFFICIAL USE ONLY

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit at auditnet@dodig.mil.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing at auditnet@dodig.mil or by mail:

Department of Defense Office of Inspector General
Office of the Deputy Inspector General for Auditing
ATTN: Audit Suggestions/13F25-04
4800 Mark Center Drive
Alexandria, VA 22350-1500

DEPARTMENT OF DEFENSE

hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline

Acronyms and Abbreviations

BTA	Business Transformation Agency
CAF	Central Adjudication Facility
CATS	Case Adjudication Tracking System
CCF	Central Clearance Facility
DA&M	Director of Administration and Management
DAMI	Department of the Army Military Intelligence
DLA	Defense Logistics Agency
DLP	Data Loss Prevention
GAO	Government Accountability Office
IAM	Information Assurance Manager
IT	Information Technology
MOA	Memorandum of Agreement
NIST SP	National Institute of Standards and Technology Special Publication
PEO	Program Executive Officer



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

APR 24 2013

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Data Loss Prevention Strategy Needed for the Case Adjudication Tracking System (Report No. DODIG-2013-072)

We are providing this report for review and comment. The Case Adjudication Tracking System did not have a data loss prevention strategy in place that included controls for identifying, monitoring, and protecting data in use and data in transit. As a result, ^{DLA: (b)}_{(7)(E)}

^{DLA: (b)}_{(7)(E)} 538 directly related to the disclosure of sensitive information. Without the proper protection of sensitive information, the system is ^{DLA: (b)(7)(E)}_{(7)(E)}

^{DLA: (b)(7)(E)} We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that recommendations be resolved promptly. The Director, Defense Logistics Agency Information Operations, Chief Information Officer, responded on behalf of the Program Executive Officer, Defense Logistics Agency. The Director's comments were responsive. However, the Director of Information Management, Department of the Army Military Intelligence, did not provide comments. Therefore, we request that the Director of Information Management, Department of the Army Military Intelligence, provide comments on Recommendations A.1.a, A.1.b, A.2.a, A.2.b, and B by May 24, 2013.

Please provide comments that conform to the requirements of DoD Directive 7650.3. If possible, send a portable document (.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) 604-8866 (DSN 664-8866).

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

DISTRIBUTION:

UNDER SECRETARY OF ACQUISITION, TECHNOLOGY, AND LOGISTICS

UNDER SECRETARY OF DEFENSE FOR POLICY

UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DOD

UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS

UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

DOD CHIEF INFORMATION OFFICER

AUDITOR GENERAL, DEPARTMENT OF THE ARMY

DIRECTOR, ADMINISTRATION AND MANAGEMENT

DIRECTOR, DEFENSE LOGISTICS AGENCY



Results in Brief: Data Loss Prevention Strategy Needed for the Case Adjudication Tracking System

What We Did

Our objective was to determine whether a data loss prevention (DLP) strategy was in place for the Case Adjudication Tracking System (CATS). Specifically, we determined whether the Defense Logistics Agency (DLA) effectively configured CATS to identify, monitor, and protect data in use, data in transit, and data at rest.

What We Found

(FOUO) Neither the Army nor DLA developed a DLP strategy for CATS that included controls for identifying, monitoring, and protecting data in use and data in transit. In addition, the Director of Information Management, Department of the Army Military Intelligence, and the Program Executive Officer (PEO), DLA did not:

- (FOUO) develop a formal security plan for CATS that identified the types of data used, how CATS interfaced with other systems, and how to store CATS data;
- (FOUO) (b) (7)(E) DLA [redacted]
- (FOUO) mitigate (b) (7)(E) DLA [redacted] DLA: (b)(7)(E)

(FOUO) This occurred because the Army inappropriately categorized CATS as a program within a larger system and therefore, did not extend the requirements for managing and protecting a DoD information system to CATS. In addition, the Army and DLA did not develop an agreement that explicitly defined the roles and responsibilities for managing and securing CATS.

(FOUO) DLA: (b)(7)(E) [redacted] (b) (7) (E)

(FOUO) (b) (7)(E) DLA [redacted]

What We Recommend

(FOUO) Among other recommendations, we recommend that the Director of Information Management, Department of the Army Military Intelligence, coordinate with the Program Executive Officer, DLA to develop a data loss prevention strategy and require independent vulnerability assessments for the CATS. (b) (7)(E) DLA

[redacted]

Management Comments and Our Response

(FOUO) The Director, Information Operations, Chief Information Officer, responded on behalf of the Program Executive Officer, DLA. DLA's comments were responsive. However, the Director of Information Management, Department of the Army Military Intelligence, did not provide comments. We request that the Director of Information Management, Department of the Army Military Intelligence, provide comments in response to the final report. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Director of Information Management, Department of the Army Military Intelligence	A.1.a, A.1.b, A.2.a, A.2.b, B	
Program Executive Officer, Defense Logistics Agency		A.2.a, A.2.b, A.3.a, A.3.b, B

Please provide comments by May 24, 2013.

Table of Contents

Introduction	1
Objective	1
Comprehensive Approach to Mitigating Data Loss	1
Case Adjudication Tracking System Developed to Adjudicate Security Clearances	1
Security Clearance Adjudication Completion Time	2
Program Management Authority of Case Adjudication Tracking System Transferred to Defense Logistics Agency	3
Expansion of Case Adjudication Tracking System Functionality and Consolidation of Central Adjudication Facilities	3
Review of Internal Controls	4
Finding A. Lack of a Data Loss Prevention Strategy Created Vulnerabilities for the Case Adjudication Tracking System	5
Data Loss Prevention Strategy Not Developed	5
(b) (7)(E) DLA	6
(b) (7)(E) DLA	6
Collective Responsibilities for Managing and Securing Case Adjudication Tracking System	7
Security Plan Did Not Exist	7
(b) (7)(E) DLA	8
(b) (7)(E) DLA	9
Lack of Defined Roles and Responsibilities	9
(b) (7)(E) DLA	10
Conclusion	10
Recommendations, Management Comments, and Our Response	11
Finding B. Production and Back-up Sites Were Not Geographically Separated	14
(b) (7)(E) DLA	14
Recommendation, Management Comments, and Our Response	15
Appendices	
A. Scope and Methodology	16
Use of Computer-Processed Data	17
Use of Technical Assistance	17
Prior Coverage	17
B. Agencies That Used Case Adjudication Tracking System	18
C. DoD Instruction 8500.2 Controls That Support a Data Loss Prevention Strategy	19
Management Comments	
Defense Logistics Agency	20

Introduction

Objective

Our objective was to determine whether a data loss prevention (DLP) strategy was in place for the Case Adjudication Tracking System (CATS). Specifically, we determined whether the Defense Logistics Agency (DLA) effectively configured CATS to identify, monitor, and protect data in use, data in transit, and data at rest.

In October 2010, the Army transferred CATS to DLA. However, the Army retained responsibility for ensuring system security compliance for the Army network. As a result, we directed recommendations to both the Army and DLA. See Appendix A for a discussion of the scope and methodology related to the objective.

Comprehensive Approach to Mitigating Data Loss

In 2008, a consortium of policymakers from the Federal Government and private sector developed 20 critical controls that would most effectively stop known cybersecurity attacks. DLP was identified as Critical Control 17, which included nine associated controls from the National Institute of Standards and Technology Special Publication (NIST SP) 800-53, "Recommended Security Controls for Federal Information Systems and Organization," August 2009. Critical Control 17 defines DLP as a comprehensive approach that identifies, monitors, and protects data in use, data in transit, and data at rest through deep content inspection and with a centralized management framework. A DLP strategy includes controls that enforce approved authorizations for controlling the flow of information within the system and between interconnected systems. NIST SP 800-53 provided guidelines that agencies must follow for selecting and specifying security controls for information systems that process, store, or transmit Federal information.

CATS Developed to Adjudicate Security Clearances

~~(FOUO)~~ CATS, originally developed in FY 2008 by the Army, is a national security adjudication case management and tracking system used by DoD agencies and other Federal agencies to adjudicate security clearances (see Appendix B). In April 2009, the Under Secretary of Defense for Intelligence designated CATS as the overall adjudication case management and security clearance adjudications system for the DoD nonintelligence community to meet requirements outlined in the Intelligence Reform and Terrorism Prevention Act of 2004. DoD¹ began modernizing the Army's existing version of CATS to meet the requirements of the Defense Industrial Security Clearance Office, the Navy, Washington Headquarters Services, the Defense Intelligence Agency, and the Air Force Central Adjudication Facilities (CAFs). From FY 2008 through FY 2011, DoD spent approximately \$28 million on CATS, and DLA plans to spend approximately \$8 million from FY 2012 through FY 2015.

¹ DoD represents the program office for the Defense Information System for Security that existed within two agencies from FY 2008 through FY 2012. The Defense Information System for Security is a family of systems that will serve as a portal to three systems that support the adjudication process, which included CATS.

(FOUO) The Army developed CATS to process requests for security clearances in an accurate and timely manner. In addition, CATS allows DoD to process over 500,000 cases annually in accordance with the timeliness and metrics established in the Intelligence Reform and Terrorism Prevention Act of 2004. (b) (7)(F) DLA

Also, CATS:

- (FOUO) receives electronic investigations from the Office of Personnel Management,
- (FOUO) automatically creates adjudication records,
- (FOUO) categorizes cases based on case type,
- (FOUO) automatically assigns and routes cases,
- (FOUO) records final security clearance determinations, and
- (FOUO) electronically transmits information to the appropriate DoD repositories.

(FOUO) The Department of the Army Military Intelligence (DAMI) integrated CATS into the Army Investigative Enterprise System, which was the single point of entry enterprise solution for personnel security investigations. The Army Investigative Enterprise System consisted of two additional systems: the Army Fingerprint System and the Personnel Security Investigation Portal System. Personnel input sensitive data onto the Standard Form 86, "Questionnaire for National Security Positions," December 2010 (SF 86), such as name, date, place of birth, social security number, past employment, and physical features. SF 86 also requires applicants to disclose information, such as:

- financial records, which includes delinquencies of debt and bankruptcies;
- drug and alcohol related treatment or counseling;
- information on family and friends;
- mental health history, including treatments; and
- civil court actions, such as family court proceedings.

Security Clearance Adjudication Completion Time

In January 2005, the Government Accountability Office (GAO) added the DoD Personnel Security Clearance Program to the GAO High Risk List because of delays in completing hundreds of thousands of background investigations and adjudications. During 2009, the Army began electronically adjudicating secret clearances through CATS, which helped to improve the processing time for adjudicating clearances. The average time to complete initial security clearance² adjudications for the Army fell from 187 days in the second quarter of FY 2009 to 10 days by the first quarter of FY 2010. In November 2010, GAO issued a report that determined significant progress was made to the DoD Personnel Security Clearance program.³ In February 2011, GAO issued a report that determined sufficient progress was made to remove the high-risk designation from the DoD Personnel Security Clearance Program.⁴

² Initial clearances involve individuals who did not have a clearance or did not receive reciprocity to honor a previously granted clearance.

³ GAO Report No. GAO-11-65, "Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum," November 19, 2010

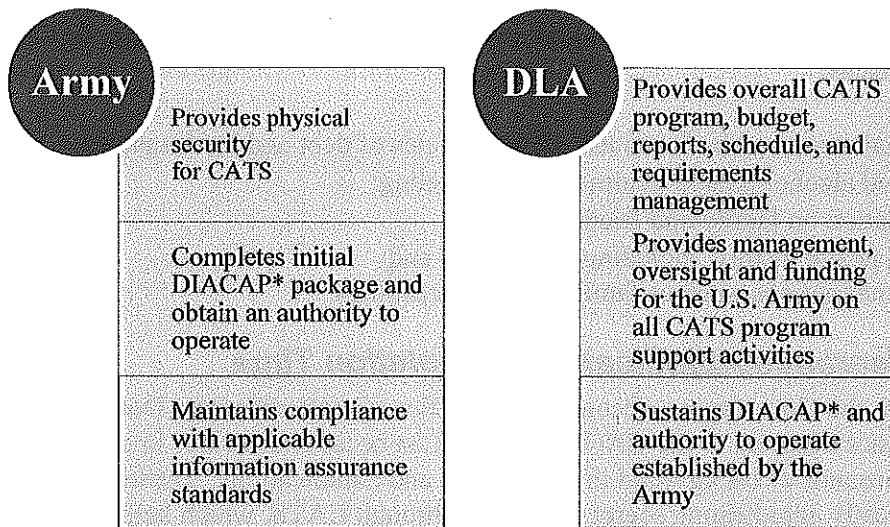
⁴ GAO Report No. GAO-11-278, "High-Risk Series: An Update," February 16, 2011

Program Management Authority of CATS Transferred to DLA

(FOUO) In October 2010, the Under Secretary of Defense for Intelligence transferred the development, operations, and maintenance of CATS from the Army to the Business Transformation Agency (BTA). CATS was transferred to BTA to ensure that CATS remained viable for all DoD CAFs. On October 1, 2011, the Secretary of Defense Efficiency Initiatives disestablished BTA and designated DLA as the agency to assume BTA responsibilities, which included the management of CATS.

(FOUO) In January 2012, the Assistant Deputy Chief of Staff, DAMI, signed a memorandum of agreement (MOA) formally outlining the transfer of program management authority to DLA. The MOA stated the Army was responsible for maintaining compliance with DoD and Federal information assurance standards until DLA moved CATS from Fort George G. Meade, Maryland, to another physical location. The Army must also provide continued and coordinated guidance on information assurance compliance to the DLA Information Assurance Manager (IAM). The MOA stated that DLA would provide management, oversight, and funding for the Army on all CATS program support activities (see the figure below).

Figure. Agency Responsibilities for CATS

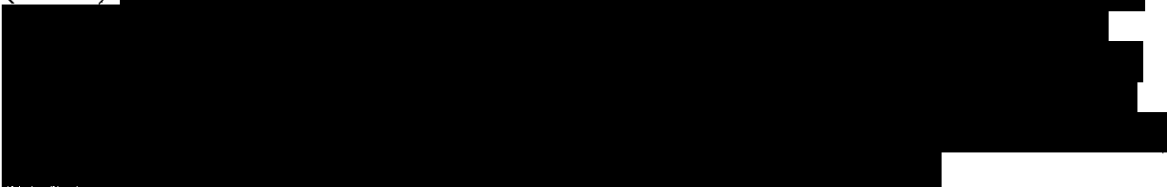


Note: The Army and DLA shared information assurance responsibilities. The finding discusses the collective responsibilities for the Army and DLA.

*DIACAP – DoD Information Assurance Certification and Accreditation Process

Expansion of CATS Functionality and Consolidation of CAFs

(FOUO) (b) (7)(E) DLA



(FOUO) In October 2010, the Deputy Secretary of Defense approved a DoD CAF consolidation. According to the Office of Deputy Secretary of Defense memorandum, "DoD Central Adjudication Facilities Consolidation," May 3, 2012, the DoD CAF consolidation will address the continuing and increasing fiscal challenges facing DoD by directing a complete consolidation of the functions, resources, and assets of the Army Central Clearance Facility (CCF), Department of Navy CAF, Air Force CAF, Washington Headquarters Services CAF, and Defense Industrial Security Clearance Office CAF to become a single organization—the DoD CAF. DoD planned to transfer all manpower, funding, and other associated resources and assets to accomplish total consolidation before FY 2014.

Review of Internal Controls

(FOUO) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We determined that internal control weaknesses existed for the Army and DLA. The Army categorized CATS as a program within a larger system and therefore, did not extend the information assurance requirements for managing and protecting DoD information system to CATS. In addition, when CATS ownership transferred to DLA, the Army and DLA did not develop an agreement that defined the roles and responsibilities for managing and securing CATS. Furthermore, the Army CCF Information Technology (IT) security manager and the DLA program manager determined that immediately establishing a back-up site was a higher priority than expending time and resources to identify a location that complied with Federal and DoD requirements. We will provide a copy of the report to the senior official responsible for internal controls at the Department of the Army and DLA.

Finding A. Lack of a DLP Strategy Created Vulnerabilities for CATS

(FOUO) Neither the Army nor DLA developed a DLP strategy for CATS that included controls for identifying, monitoring, and protecting data in use and data in transit. The Army took action to protect its network by implementing encryption mechanisms and boundary protections. However, the Army did not (b)(7)(E) DLA for CATS. In addition, the Director of Information Management, DAMI, and the Program Executive Officer (PEO), DLA did not:

- (FOUO) develop a formal security plan for CATS that identified the types of data used, how CATS interfaced with other systems, and how to store CATS data;
- (FOUO) (b)(7)(E) DLA ; or
- (FOUO) mitigate (b)(7)(E) DLA DLA: (b)(7)(E)

(FOUO) This occurred because the Army inappropriately categorized CATS as a program within a larger system and therefore, (b)(7)(E) DLA

(b)(7)(E) DLA In addition, the Army and DLA did not develop an agreement that explicitly defined the roles and responsibilities for managing and securing CATS.

(FOUO) (b)(7)(E) DLA

(FOUO) Without an effective DLP strategy for CATS, (b)(7)(E) DLA


DLP Strategy Not Developed

(FOUO) When the Army developed CATS in FY 2008, the Director of Information Management, DAMI, did not develop a strategy that included controls for identifying, monitoring, and protecting CATS. In addition, the Director of Information Management, DAMI, did not coordinate with the DLA PEO to develop a DLP strategy for CATS. According to NIST SP 800-53, organizations should:

- use encryption to protect data in use,
- protect data transmitted across internal and external networks,
- monitor and control communications at the external boundary of the system,
- monitor communications for unusual or unauthorized activity within the system,
- develop an enterprise architecture that considers information security risks, and
- protect the confidentiality and integrity of data at rest (see Finding B).

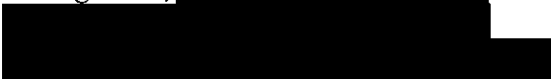
Army Implemented Encryption Mechanisms and Boundary Protections

(FOUO) The Army implemented controls to protect its network. The Army used encryption to protect CATS data in use through public key infrastructure.⁵ Specifically, the Army implemented DoD-compliant encryption controls that required users of CATS to use common access cards or personal identity verification cards to access the system. In addition, the Army protected data in transit using virtual private networks for remote access. (b) (7)(E) DLA



No Strategy for Independently Assessing Vulnerabilities and Monitoring System Activity

(FOUO) The Director of Information Management, DAMI, did not develop a DLP strategy for CATS that included controls for identifying, monitoring, and protecting data in use and data in transit. In addition, the Director of Information Management, DAMI, did not coordinate with the DLA PEO to develop a DLP strategy to protect the data in CATS. According to Army Regulation 25-2, "Information Assurance," March 23, 2009, (AR 25-2), the Assistant Deputy Chief of Staff, DAMI, is responsible for implementing information assurance requirements and planning the operation of information assurance strategies. In addition, AR 25-2 requires commands to conduct vulnerability assessments on all systems to identify residual vulnerabilities and provide risk mitigation strategies for those vulnerabilities before fielding or installing systems. Since the Director of Information Management, DAMI, did not develop a DLP strategy, the Army CCF IAM did not implement information assurance controls for capturing system activities and performing vulnerability assessments. According to the Army CCF IAM, the Army "divorced" themselves from CATS and therefore, did not actively coordinate the development of a DLP strategy with DLA. For example, the Director of Information Management, (b) (7)(E) DLA



The Director of Information Management, DAMI, did not develop a DLP strategy because the Army did not consider CATS an information system.

Instead, the Army inappropriately categorized CATS as a program within the Army Investigative Enterprise System and therefore, did not extend information assurance requirements to CATS for managing and securing the system.

(FOUO) (b) (7)(E) DLA



⁵ Public Key Infrastructure is a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

⁶ (b) (7)(E) DLA



~~FOR OFFICIAL USE ONLY~~

According to AR 25-2, an information system processes, collects, maintains, uses, shares, disseminates, and reports information. In contrast, according to the "Federal Information System Controls Audit Manual," February 2009, a program is a set of instructions that, when followed and executed by a computer, performs a task. CATS:

- (FOUO) collects and maintains electronic investigations from the Office of Personnel Management,
- (FOUO) processes adjudication data and automatically assigns and routes cases,
- (FOUO) records final security clearance determinations, and
- (FOUO) electronically disseminates information to the appropriate DoD repositories.

(FOUO) The Army should have (b)(7)(E) DLA [REDACTED] Without a DLP strategy for CATS, the Army increased its risk of not appropriately assessing security risks, identifying vulnerabilities, and implementing the appropriate controls to prevent data loss (b)(7)(E) DLA [REDACTED]

Therefore, the Director of Information Management, DAMI, in coordination with the DLA PEO, should develop a DLP strategy that includes requirements for (b)(7)(E) DLA [REDACTED]

[REDACTED] In addition, the Director of Information Management, DAMI, should require an independent vulnerability assessment for CATS before allowing the system to connect to the Army's network.

Collective Responsibilities for Managing and Securing CATS

(FOUO) When DLA assumed responsibility for CATS in January 2012, the Army retained a level of responsibility for securing CATS since the system resided on an Army network. Additionally, as the owner of CATS, DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003 (DoDI 8500.2), requires the DLA PEO to provide guidance for developing and maintaining information systems to ensure risks are mitigated. Therefore, the Army and DLA have collective responsibilities. However, the Army and DLA did not:

- (FOUO) develop a plan that identified the types of data used within CATS, how CATS interfaced with other systems, and data stored on CATS;
- (FOUO) (b)(7)(E) DLA [REDACTED]
- (FOUO) develop a methodology for identifying, correcting, and mitigating security vulnerabilities to ensure the protection of data in use.

Security Plan Did Not Exist

(FOUO) The Director of Information Management, DAMI, and the DLA PEO did not develop a formal security plan for CATS that identified the types of data used within CATS, how CATS interfaced with other systems, and how to store CATS data. According to NIST SP 800-53, organizations must develop a formal security planning policy that addresses the roles and responsibilities, management commitment, and coordination among other entities. However, neither agency developed a security plan for CATS that identified an accurate enterprise architecture in relation to CATS and listed the types of data used by CATS.

~~FOR OFFICIAL USE ONLY~~

(FOUO) (b) (7)(E) DLA
[Redacted]

(FOUO) (b) (7)(E) DLA
[Redacted]

The Director of Information Management, DAMI, and the DLA PEO should develop a system security plan that includes information on the type of data used with CATS, interfaces with other system, and the storage of systems data.

(b) (7)(E) DLA
(FOUO) (b) (7)(E) DLA
[Redacted]

(FOUO) (b) (7)(E) DLA
[Redacted]

(b) (7)(E) DLA
[Redacted]

(b) (7)(E) DLA

(FOUO) The Army CCF IT security manager and the DLA program manager did not develop a formal agreement for identifying, correcting, and mitigating security vulnerabilities.

(b) (7)(E) DLA

DoDI 8500.2 requires agencies to develop a comprehensive vulnerability management process that includes identifying and mitigating existing vulnerabilities. The Army and DLA were responsible for identifying, correcting, and mitigating CATS vulnerabilities. (b) (7)(E) DLA

(FOUO) (b) (7)(E) DLA

(FOUO) (b) (7)(E) DLA

The Director of Information Management, DAMI, and the DLA PEO should develop an agreement that, at a minimum, explicitly defines the roles and responsibilities for managing and securing CATS, monitoring system events, identifying security vulnerabilities, and implementing mitigating controls to correct vulnerabilities.

Lack of Defined Roles and Responsibilities

(FOUO) The Director of Information Management, DAMI, and the DLA PEO did not develop an agreement that explicitly defined the responsibilities for managing and securing CATS as required by NIST SP 800-53. Therefore, neither agency identified the types of data CATS used, systems that interface with CATS, and storage requirements for CATS data. In addition, the Army and DLA did not (b) (7)(E) DLA. Furthermore, the Army and DLA did not (b) (7)(E) DLA

Without an agreement detailing roles and responsibilities, neither agency understood the security expectations for CATS, which increased the risk that the Army and DLA would not

⁸ Results discussed in this report do not include scan results from the Security Content Automation Protocol validation tool.

(FOUO) implement the necessary security controls to properly protect CATS and its data. ^{DLA:}
(b)(7)(E) DLA

[REDACTED]. The Director of Information Management, DAMI, and the DLA PEO should develop an agreement that, at a minimum, explicitly defines the roles and responsibilities for managing and securing CATS, monitoring system events, identifying security vulnerabilities, and implementing and mitigating controls to correct vulnerabilities.

DLA: (b)(7)(E)

(FOUO) DLA: (b)(7)(E)

[REDACTED] According to NIST SP 800-53, organizations should manage information system accounts by identifying account types and authorized users, specifying access privileges, granting access, and reviewing accounts. ^{DLA: (b)(7)(E)}

[REDACTED]

Conclusion

(FOUO) The Army and DLA did not develop a DLP strategy for CATS that included controls for identifying, monitoring, and protecting data in use and data in transit. For example, ^{(b)(7)(E) DLA}
[REDACTED]. In addition, the Army and DLA did not:

- (FOUO) develop a formal security plan for CATS that identified the types of data used, how CATS interfaced with other systems, and how to store CATS data;
- (FOUO) ^{DLA: (b)(7)(E)} [REDACTED]
- (FOUO) ^{DLA: (b)(7)(E)} [REDACTED]

(FOUO) ^{DLA: (b)(7)(E)} [REDACTED]

DLA: (b)(7)(E)

⁹ The six participating CAFs are the Army, Defense Industrial Security Clearance Office, the Navy, Washington Headquarters Services, the Defense Intelligence Agency, and the Air Force.

(FOUO) DLA: (b)(7)(E)

Recommendations, Management Comments, and Our Response

(FOUO) A.1. We recommend that the Director of Information Management, Department of the Army Military Intelligence:

a. (FOUO) Coordinate with the Defense Logistics Agency to develop a data loss prevention strategy that includes

DLA: (b)(7)(E)

b. (FOUO)

DLA: (b)(7)(E)

Management Comments Required

The Army did not provide comments to these recommendations. Although administrative responsibilities for CATS was transferred to Director of Administration and Management (DA&M), CATS still resides on the Army network. As a result, the Army still retains responsibility for securing CATS by updating patches, ensuring network availability and connectivity, and resolving network issues. Therefore, we request that the Director of Information Management, Department of the Army Military Intelligence, provide comments by May 24, 2013.

(FOUO) A.2. We recommend that the Director of Information Management, Department of the Army Military Intelligence, and the Program Executive Officer, Defense Logistics Agency:

a. (FOUO) Develop a system security plan that includes information on the type of data used with the Case Adjudication Tracking System, interfaces with other system, and the storage of systems data.

b. (FOUO) Develop an agreement that, at a minimum, explicitly defines the roles and responsibilities for managing and securing the Case Adjudication Tracking System, monitoring system events, identifying security vulnerabilities, and implementing mitigating controls to correct vulnerabilities.

Management Comments Required

The Army did not provide comments to these recommendations. Although administrative responsibilities for CATS were transferred to Director of Administration and Management (DA&M), CATS still resides on the Army network. As a result, the Army still retains responsibility for securing CATS by updating patches, ensuring network availability and connectivity, and resolving network issues. Therefore, we request that the Director of Information Management, Department of the Army Military Intelligence, provide comments by May 24, 2013.

DLA Comments

(FOUO) The Director, Defense Logistics Agency Information Operations, Chief Information Officer, responded on behalf of the Program Executive Officer, Defense Logistics Agency, and agreed with the recommendations. According to the Director, the five DoD Central Adjudication Facilities were consolidated into a single organization, which resulted in the responsibilities of the DAMI being transferred to the DA&M. The Director stated that DLA would work with DA&M to develop corrective actions by December 20, 2013. Specifically, the Director stated that DLA would develop a system security plan that includes information on the type of data, interfaces with other system, and the storage of systems data. In addition, the Director stated DLA would work with the Director of Administration and Management and the DoD CAF to develop an agreement that defined the roles and responsibilities for managing and securing CATS, monitoring system events, identifying security vulnerabilities, and implementing mitigating controls to correct vulnerabilities.

Our Response

(FOUO) The Director's comments were responsive. Although the Director stated DLA would work with the DA&M instead of the Army, we agree that DA&M would also be involved in the development of an agreement that defines roles and responsibilities. The CAFs were consolidated to the DoD CAF, which is under the authority, direction, and control of DA&M. Therefore, no further comments are required.

(FOUO) A.3. We recommend that the Program Executive Officer, Defense Logistics Agency:

a. (FOUO) ^{DLA: (b)(7)(E)} [REDACTED]

b. (FOUO) ^{DLA: (b)(7)(E)} [REDACTED]

DLA Comments

(FOUO) The Director, Defense Logistics Agency Information Operations, Chief Information Officer, responded on behalf of the Program Executive Officer, Defense Logistics Agency, and agreed with the recommendations. ^{DLA: (b)(7)(E)} [REDACTED]

Our Response

(FOUO) The Director's comments were responsive. Although the Director stated DLA would work with the DA&M instead of the Army, we agree that DA&M would also be involved in the

~~FOR OFFICIAL USE ONLY~~

(FOUO) development of an agreement that defines roles and responsibilities. The CAFs were consolidated to the DoD CAF, which is under the authority, direction, and control of DA&M. Therefore, no further comments are required.

~~FOR OFFICIAL USE ONLY~~

Finding B. Production and Back-up Sites Were Not Geographically Separated

(FOUO) The Army and DLA inappropriately established a back-up site for CATS servers that were within the same geographic region as the primary production servers. This occurred because the Army and DLA decided that immediately establishing a back-up site was a higher priority than expending time and resources to identify a location that complied with Federal and DoD requirements. As a result, the Army and DLA increased the risk that CATS, and all data in the system, could be lost if a manmade or natural disaster affected the region.

Back-up Servers [DLA: (b)(7)(E)] Miles From Production Servers

(FOUO) The Army CCF IT security manager and the DLA program manager established a back-up site for the servers that support CATS [DLA: (b)(7)(E)] miles of the production server. In addition, the Army CCF IT security manager and the DLA program manager did not request Designated Approving Authority approval to select [DLA: (b)(7)(E)] NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems," May 2010, requires organizations to identify alternate storage sites that are geographically separated from the primary site to avoid being affected by the same disaster. DoDI 8500.2 validation procedures state organizations should ensure back-up media is stored at a Designated Approving Authority approved offsite location. When the Army began using CATS in FY 2007, the Army CCF IT security manager made the decision to locate the back-up servers [DLA: (b)(7)(E)] [redacted]

(FOUO) The Army recognized the need to move the back-up servers and planned to move them to Fort Belvoir, Virginia, in FY 2010, although the base was not outside of the geographical region. However, the Army was unable to move the back-up servers to Fort Belvoir because the site did not meet the environmental control requirements to sustain a back-up site.

(FOUO) The Army CCF IT security manager and the DLA program manager determined that standing up an operational back-up site within a reasonable timeframe was more important than expending time and resources to establish a back-up site outside of the geographic disaster zone. Therefore, the Army CCF IT security manager and the DLA program manager allowed the back-up servers to remain at [DLA: (b)(7)(E)] without obtaining a waiver from the Designated Approving Authority. If a disaster destroys the production and back-up servers, the integrity of the data at rest will be compromised, and DoD personnel security clearances could take [DLA: (b)(7)(E)] to adjudicate. In addition, there was an increased risk DoD could return to the GAO High Risk List for personnel security clearances. Therefore, the Army and DLA should immediately move the back-up servers to an approved location outside of the geographic region that complies with Federal and DoD information assurance requirements. If moving the back-up servers is not immediately feasible, request an interim waiver from the Designated Approving Authority and develop a time-phased plan to move the back-up servers outside of the geographic region.

Recommendation, Management Comments, and Our Response

~~(FOUO)~~ B. We recommend that the Director of Information Management, Department of the Army Military Intelligence, and the Program Executive Officer, Defense Logistics Agency, immediately move the back-up servers to an approved location outside of the geographic region that complies with Federal and DoD information assurance requirements. If moving the back-up servers is not immediately feasible, request an interim waiver from the Designated Approving Authority and develop a time-phased plan to move the back-up servers outside of the geographic region.

Management Comments Required

The Army did not provide comments to these recommendations. Although administrative responsibilities for CATS was transferred to Director of Administration and Management (DA&M), CATS still resides on the Army network. As a result, the Army still retains responsibility for ensuring the physical security of CATS back-up servers. Therefore, we request that the Director of Information Management, Department of the Army Military Intelligence, provide comments by May 24, 2013.

DLA Comments

~~(FOUO)~~ The Director, Defense Logistics Agency Information Operations, Chief Information Officer, responded on behalf of the Program Executive Officer, Defense Logistics Agency, and agreed with the recommendations. The Director stated that DLA would develop a plan and funding to move the disaster recovery site outside of the National Capital Region. The Director stated DLA is in the process of procuring equipment to establish a disaster recovery site in Monterey, California, at the Defense Manpower Data Center. In addition, the Director stated DLA would request a waiver from the Designating Approving Authority. Furthermore, DLA plans to develop a time-phased approach to move the back-up servers by July 22, 2013.

Our Response

The Director's comments were responsive. Therefore, no further comments are required.

Appendix A. Scope and Methodology

(FOUO) We conducted this performance audit from April 2012 through February 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.

(FOUO) Based on our audit objective, we intended to focus the audit on DLA. However, during the audit, we found that the Army developed CATS to support the Army CCF and the Army CCF has a responsibility to maintain compliance with applicable information assurance standards until CATS is moved to DLA. As a result, the scope of the audit included the Army and DLA because these agencies were responsible for the security of CATS. To determine whether a DLP strategy was in place for CATS, we interviewed personnel from the Army and DLA to obtain information on the controls in place to prevent data loss for CATS. In addition, we reviewed system security policies and procedures from the Army and DLA to determine whether the agencies complied with information assurance requirements.

We reviewed the following seven NIST SP 800-53 controls that support a DLP strategy.

- Information Flow Enforcement requires CATS to enforce approved authorizations for controlling the flow of information within the systems and between interfaces.
- Enterprise Architecture requires the Army and DLA to develop an enterprise architecture that considers information security and the risks associated with system.
- Boundary Protection requires CATS to monitor and control communications at the external boundaries.
- Transmission Confidentiality requires CATS to protect the information transmitted.
- Use of Cryptography requires CATS to implement required cryptography protections.
- Information System Monitoring requires the Army and DLA to monitor system events and detect system attacks.
- Protection of Information at Rest requires CATS protect the confidentiality and integrity of information at rest.

Although Critical Control 17 listed media access and media storage as additional controls that support a DLP strategy, we did not review these controls because CATS did not use digital media (such as diskettes, removable hard drives, and flash drive) and therefore, did not require storage of such devices.

In addition, we reviewed 34 DoDI 8500.2 controls that supplemented the NIST SP 800-53 controls related to system continuity, security design and configuration, enclave boundary defense, enclave and computing environment, physical and environmental controls, and vulnerability management (see Appendix C for list of controls). To validate the existence of these controls, we asked the Army and DLA to explain how each agency applied validation procedures for each control. We also analyzed documents the Army and DLA provided as evidence of controls. We used the information obtained from interviews and supporting documents to conclude on whether DLP controls existed and functioned properly.

(FOUO) Furthermore, we requested the Army and DLA run vulnerability scans for the servers that directly support CATS. ^{DLA: (b)(7)(E)}

(FOUO) During interviews, the Army and DLA could not provide adequate evidence that a formal DLP strategy existed and that the Army and DLA implemented appropriate controls to support a DLP strategy. ^{(b)(7)(E) DLA}

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Use of Technical Assistance

The DoD OIG Information Systems Directorate assisted with the audit. These personnel assisted with the understanding of DLP controls for DoD systems. The Information Systems Directorate also provided a crosswalk between DoDI 8500.2 and NIST SP 800-53 controls to further assist in determining the appropriate controls that support DLP.

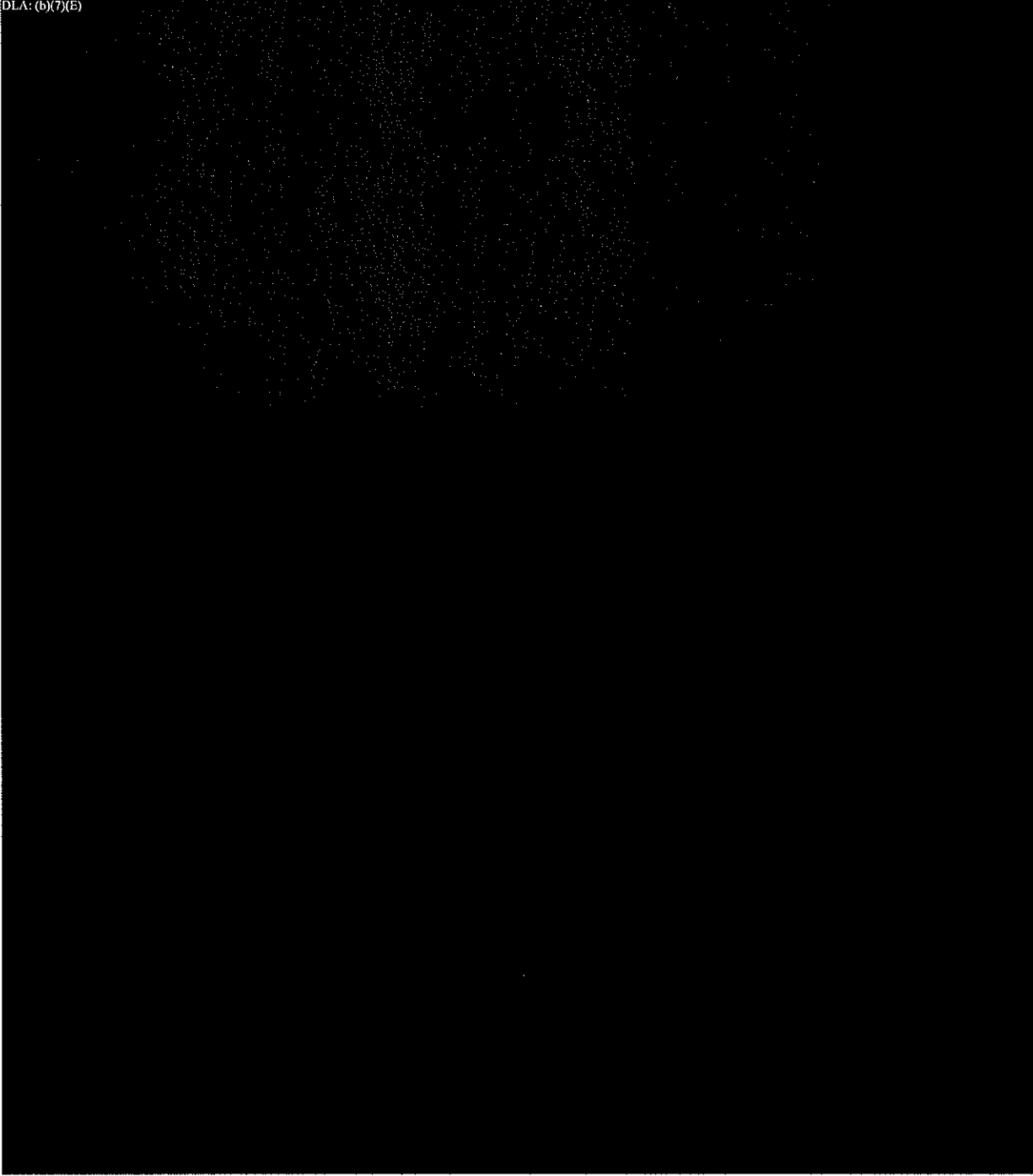
Prior Coverage

No prior coverage has been conducted on CATS during the last 5 years.

Appendix B. Agencies That Used CATS

The following graphic shows DoD and non-DoD agencies that used CATS to adjudicate security clearances.

DLA: (b)(7)(E)



Source: DLA

Appendix C. DoD Instruction 8500.2 Controls That Support a DLP Strategy

Control No.	Control Name
COAS-2	Alternate Site Designation
COBR-1	Protection of Background and Restoration Assets
CODB-1	Data Back-up Procedures
COSW-1	Backup Copies of Critical Software
DCBP-1	Best Security Practices
DCFA-1	Functional Architecture for AIS Applications
DCID-1	Interconnection Documentation
DCMC-1	Mobile Code
DCNR-1	Non-repudiation
DCPA-1	Partitioning the Application
DCPP-1	Ports, Protocols, and Services
DCSD-1	IA Documentation
EBBD-2	Boundary Defense
EBCR-1	Connection Rules
EBRP-1	Remote Access for Privileged Functions
EBRU-1	Remote Access for User Functions
EBVC-1	VPN Controls
ECAN-1	Access for Need-to-Know
ECAR-2	Audit Record Content
ECAT-2	Audit Trail, Monitoring, Analysis and Reporting
ECCD-2	Changes to Data
ECCR-1	Encryption for Confidentiality (Data at Rest)
ECCT-1	Encryption for Confidentiality (Data in Transit)
ECIC-1	Interconnections among DoD Systems and Enclaves
ECID-1	Host Based IDS
ECLO-1	Logon
ECNK-1	Encryption for Need-To-Know
ECPA-1	Privileged Account Control
ECVP-1	Virus Protection
IAAC-1	Account Control
PECF-1	Access to Computing Facilities
PESL-1	Screen Lock
PESS-1	Storage
VIIR-1	Incident Response Planning

Defense Logistics Agency Comments



DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

MAR 27 2013

MEMORANDUM FOR DLA OFFICE OF THE INSPECTOR GENERAL

ATTN: ^{DoD OIG (b)(6)} [REDACTED]

SUBJECT: Draft Audit Report: Data Loss Prevention Strategy Needed for the Case Adjudication Tracking System (Project No. D2012-D000LC-0148.000), dated February 25, 2013

The DLA Information Operations staff has reviewed the draft audit report. Management comments and actions associated with the findings and recommendations are outlined on the attachment.

The administrative point of contact is [REDACTED] DLA Information Operations, IT Business, Licensing, and Performance Management, at [REDACTED] or email: [REDACTED]

[REDACTED]
KATHY CUTLER
Director, DLA Information Operations
Chief Information Officer

Attachment:
As stated

Response to DoDIG Report on "Data Loss Prevention Strategy Needed for the Case Adjudication Tracking System", (Project No. D2012-D000LC-0148,000)

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

The five DoD Central Adjudication Facilities (CAF) have been consolidated into a single organization. The consolidation has resulted in the responsibilities of the Director of Information Management, Department of the Army Military Intelligence (DAMI) transferring to the Director of Administration and Management (DA&M).

Recommendation A.2. We recommend that the Director of Information Management, Department of the Army Military Intelligence, and the Program Executive Officer, Defense Logistics Agency:

- a) Develop a system security plan that includes information on the type of data used with the Case Adjudication Tracking System, interfaces with other system, and the storage of systems data.
- b) Develop an agreement that, at a minimum, explicitly defines the roles and responsibilities for managing and securing the Case Adjudication Tracking System, monitoring system events, identifying security vulnerabilities, and implementing mitigating controls to correct vulnerabilities.

Response: Concur. DLA J6 Management will work with DA&M to develop corrective actions to address all recommendations specific to DLA by December 20, 2013:

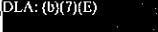

- DLA J6 Management will work with DA&M to develop the system security plan that includes information on the type of data, interfaces with other system, and the storage of systems data for the Case Adjudication Tracking System (CATS).
- DLA J6 Management will work with DA&M and the DoD CAF to develop an agreement to define the roles and responsibilities for managing and securing the Case Adjudication Tracking System, monitoring system events, identifying security vulnerabilities, and implementing mitigating controls to correct vulnerabilities.

Recommendation A.3. We recommend that the Program Executive Officer, Defense Logistics Agency:

- a)  DLA: (b)(7)(E)
- b)  DLA: (b)(7)(E)

Response: Concur. DLA J6 Management will develop corrective actions by December 20, 2013:

-  DLA: (b)(7)(E)

- That will create policy and processes with DA&M so that the Defense Information System for Security (DISS) IAM, which includes oversight of CATS, has the capability ^{DLA: (S)(7)(E)} 


Recommendation B.1 We recommend that the Director of Information Management, Department of the Army Military Intelligence, and the Program Executive Officer, Defense Logistics Agency, immediately move the back-up servers to an approved location outside of the geographic region that complies with Federal and DoD information assurance requirements. If moving the back-up servers is not immediately feasible, request an interim waiver from the Designated Approving Authority and develop a time-phased plan to move the back-up servers outside of the geographic region.

Response: Concur. DLA J6 Management will develop a plan and funding to move the disaster recover site outside the National Capital Region.

- DLA J6 Management is currently in the process of procuring equipment to deploy to the Defense Manpower Data Center (DMDC) Monterey, CA in order to establish a disaster recover site outside the National Capital Region complying with Federal and DoD information assurance requirements. A waiver will be requested from the Designated Approving Authority and a time-phased plan to move the back-up servers outside of the geographic region will be developed by July 22, 2013.

FOR OFFICIAL USE ONLY



Inspector General
Department of Defense

FOR OFFICIAL USE ONLY