Description of document:	Six (6) Defense Logistics Agency (DLA) Audits, 2011-2015
Requested date:	29-February-2016
Released date:	31-October-2016
Posted date:	05-December-2016
Source of document:	Freedom of Information Act Request DLA Headquarters ATTN: DGA 8725 John J. Kingman Road, Suite 1644 Fort Belvoir, VA 22060-6221 Fax: 703-767-6091 E-mail: hq-foia@dla.mil

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

OCT 31 2016

This letter responds to your February 29, 2016, Freedom of Information Act request for various DLA audits. Specifically, DLAOIG-FY-15-05, DLAOIG-FY15-06, DLAOIG-FY15-07, DLAOIG-FY15-09, DLAOIG-FY15-10, DLAOIG-FY16-01, DLAOIG-FY16-05, DAF-12-15, DAO-12-07, and DAO-10-21.

Please find the enclosed CD with records released to you in full. After discussions with our FOIA office, you withdrew a portion of your request pertaining to DLAOIG-FY15-09, Defense Agencies Initiative. Additionally, DLA Audits, DLAOIG-FY16-01 and DLAOIG-FY16-05 are withheld in their entirety pursuant to FOIA exemption 5 U.S.C. §552 (b)(5), deliberative process privilege. Exemption b(5) protects inter-agency and intra-agency material which would not be available by law to a party other than an agency in litigation with the agency. DLA is invoking the "deliberative process" privilege interagency material which could reveal the agency's vulnerabilities.

Additionally, DLAOIG-FY15-10, Defense Travel System (DTS) is no longer under our agency's cognizance as it has been transferred to Defense Manpower Data Center. We referred this portion of your request to their FOIA Office. They may be reached at:

OSD/JS FOIA Requester Service Center, Office of Freedom of Information
1155 Defense Pentagon
Washington, DC 20301-1155
(866) 574-4970 (Telephone)
(571) 372-0500 (Fax)
whs.mc-alex.esd.mbx.osd-js-foia-requester-service-center@mail.mil

You have the right to appeal this partial denial. An appeal must be made in writing to the General Counsel and reach the General Counsel's Office within 90 calendar days from the date of this letter, and no later than 5:00 pm Eastern Standard Time. The appeal should include your reasons for reconsideration and enclose a copy of this letter. An appeal may be mailed, emailed to hq-foia@dla.mil, or faxed to 703-767-6091. Appeals are to be addressed to the General Counsel, Defense Logistics Agency, ATTN: DGA, Suite 1644, 8725 John J. Kingman Road, Fort Belvoir, Virginia 22060-6221.

No fees are being charged. Should you have any questions or require further information, please contact Ms. Kathy Dixon at 703-767-6183 or kathy.dixon@dla.mil. Please reference our case number DLA-16-HFOI-00055, in any subsequent communication regarding this request.

Sincerely,

Steven Pigott

STEVEN PIGOTT
Deputy IG for Audit

Enclosure:
as stated

DLA Office of the Inspector General

Audit of DLA Disposition Services Contingency Operations in Afghanistan

Audit Report: DAO-12-07 **January 15, 2013**

Executive Summary

Audit Report DAO-12-07
January 15, 2013

Audit of DLA Disposition Services Contingency Operations in Afghanistan

Results

DLA Disposition Services supports the Warfighter and protects the public by providing worldwide disposal management solutions. Specific to contingency operations, DLA Disposition Services' primary mission is to reutilize or safely and securely dispose of excess military equipment and material.

DLA Disposition Services generally had sufficient policies and controls in place to accomplish the mission. We reviewed DLA Disposition Services operations at the three sites in Afghanistan, specifically the receipt and demilitarization processes, property reutilization, scrap removal, site access controls, and backlog processing.

The three DLA Disposition Services sites typically conducted operations concerning property receipt, demilitarization, reutilization, and backlog processing in accordance with existing DOD and DLA policies. For example, most sites allowed only authorized personnel to reutilize property, and we observed all sites properly perform the physical demilitarization of items.

We also reviewed the utilization and distribution of resources, to include the Expeditionary Disposal Remediation Team (ERDT), support contracts, and equipment. DLA Disposition Services recently established an equipment maintenance contract to address equipment challenges unique to Afghanistan. EDRTs deployed in Afghanistan frequently visited forward operating bases, as intended by the program.

However, policies and controls related to the theater-specific mission and challenges should be strengthened and improved, particularly to increase assurance of mission success throughout drawdown operations. Our audit yielded weaknesses in the controls related to scrap operations, demilitarization records and coding, contracts, and the EDRT mission. Additionally, personnel occasionally deviated from the overarching DOD and DLA policies governing operations due to established practices in the theater environment.

This occurred because there was no theater-specific guidance in place and a lack of standardized training requirements for all personnel involved in DLA Disposition Services operations.

As a result, DLA Disposition Services may not be able to provide optimal support to the Warfighter and may not be best postured to handle future drawdown support requirements.

The development and implementation of theater-specific guidance would give DLA Disposition Services the opportunity to emphasize important aspects of operations occurring in Afghanistan, and would help ensure processes are standardized. This would allow for easier monitoring by leadership and greater accountability by DLA employees and contractors alike.

Why DLA OIG Did this Review

The audit was included in the DLA OIG Fiscal Year 2012 Audit and Crime Vulnerability Assessment Plan under the DLA Strategic Goal of supporting operational requirements and force drawdown/equipment reset processes in the Southwest Asia theater. The DLA risk assessment, championed by J5, identified the unauthorized release of controlled property as a significant risk area.

Additionally, the Operational Evaluation Team report, released in April 2010, identified potential vulnerabilities in DLA Disposition Services operational areas in Afghanistan.

What DLA OIG Did

Our audit objective was to evaluate DLA Disposition Services operations in Afghanistan. Specifically, to determine whether DLA Disposition Services had sufficient policies and controls in place to accomplish the mission and to address theater-specific challenges.

What DLA OIG Recommends

This report contains 12 recommendations addressed to the Director, DLA Disposition Services. Recommendations include:

- Develop guidance specific to operations in Afghanistan and ensure existing policies are followed at the sites.
- Identify training for all pre-deployed personnel to receive in order to ensure employees understand most position requirements and to create a cross-leveled workforce.
- Develop and implement standard operating procedures for the EDRT program, to include program expectations, metrics to measure success, and examples of standardized reports and training materials for the sites.

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

January 15, 2013

MEMORANDUM FOR DLA DISPOSITION SERVICES

SUBJECT: Final Report on Audit of DLA Disposition Services Contingency Operations in Afghanistan

This is our report on the audit of DLA Disposition Services Contingency Operations in Afghanistan. It includes the results of our audit and conclusions concerning the policies and controls in place to effectively accomplish the mission.

Our main objective was to evaluate DLA Disposition Services operations in Afghanistan. Specifically, to determine whether sufficient policies and controls were in place to accomplish the mission and to address theater-specific challenges. Generally, DLA Disposition Services established sufficient policies and controls to accomplish the mission. However, policies and controls related to the theater-specific mission and challenges should be strengthened and improved, particularly to increase assurance of mission success throughout drawdown operations. This report contains 12 recommendations addressed to the Director of DLA Disposition Services to improve DLA Disposition Services operations throughout Afghanistan. Management officials fully concurred with the issues and recommendations discussed in this report, and actions planned are responsive to the issues. Verbatim management comments are included in Appendix D of this report.

We appreciate the courtesies and cooperation extended to us during the audit. For additional information about this report, contact Ms. Jessy Joseph @ (703) 767-7494 or email at jessy.joseph@dla.mil.

Steven D Pigott

STEVEN D. PIGOTT
Deputy Inspector General
DLA OIG Audit Division

CONTENTS

Page

Introduction

Results, Recommendations, and Conclusions

Appendices

INTRODUCTION

OBJECTIVES, SCOPE, AND METHODOLOGY

The DLA Office of the Inspector conducted an audit to determine whether DLA Disposition Services had sufficient policies and controls in place to accomplish the mission and to address theater-specific challenges.

We analyzed Management Information Distribution and Access System (MIDAS) property receipt transaction data for all three DLA Disposition Services sites in Afghanistan occurring between January 1 and March 29, 2012. We randomly selected 45 receipt transactions from each site with demilitarization (DEMIL) codes B, C, D, E, F, and Q (codes that identify items requiring mutilation or demilitarization), as well as two DEMIL A transactions (indicating no mutilation or demilitarization required) per site. We did not assess the reliability of the computer-generated data because we reviewed source documentation maintained at the sites to develop the related audit conclusions.

We conducted this performance audit in accordance with generally accepted government auditing standards issued by the Government Accountability Office except for the standard related to organizational independence. This organizational impairment resulted from the DLA Office of the Inspector General Audit Division (formally DLA Accountability Office Audit Division) not being accountable to the head or deputy head of DLA, and conducting non-audit services related to Office of Management and Budget Circular A-123, Appendix A, Management's Responsibility for Internal Control. To correct this, we established policies and procedures to provide reasonable assurance of conforming to applicable professional standards. However, the impairment had no effect on the quality of this report as generally accepted government auditing standards requires that we plan and conduct the performance 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.

To determine whether sufficient policies and controls were in place, we:

- Reviewed regulations and guidance related to DLA Disposition Services operations.

- Interviewed personnel responsible for DLA Disposition Services contingency operations.

- Interviewed personnel participating in DLA Disposition Services contingency operations.

- Analyzed receipt (turn-in) transactions and supporting documentation based on a sample from MIDAS for turn-ins occurring between January 1, 2012 and March 29, 2012.

- Conducted on-site observations of the receipt, demilitarization, backlog, scrap removal, and yard access procedures at the three DLA Disposition Services sites in Afghanistan during April 2012.

- Analyzed personnel rosters, equipment status lists, and related contracts to determine if sites had sufficient resources to perform the mission.

- Obtained and reviewed Expeditionary Disposal Remediation Team (EDRT) documentation, to include after action reports, forward operating base (FOB) assessments, situational awareness reports, daily muster reports, utilization spreadsheets, and draft guidance.

BACKGROUND

DLA Disposition Services supports the Warfighter and protects the public by providing worldwide disposal management solutions. Specific to contingency operations, DLA Disposition Services' primary mission is to reutilize or safely and securely dispose of excess military equipment and material. To accomplish this mission in the Afghanistan contingency environment, DLA Disposition Services operated three disposition sites, with plans for a fourth site, and regularly deployed personnel to assist with disposal operations throughout Afghanistan. DLA Disposition Services identified lessons learned from the Iraq drawdown mission, which included:

- Surge of DEMIL-required property and vehicles.

- Timely equipment maintenance.

- Base access issues with contractors.

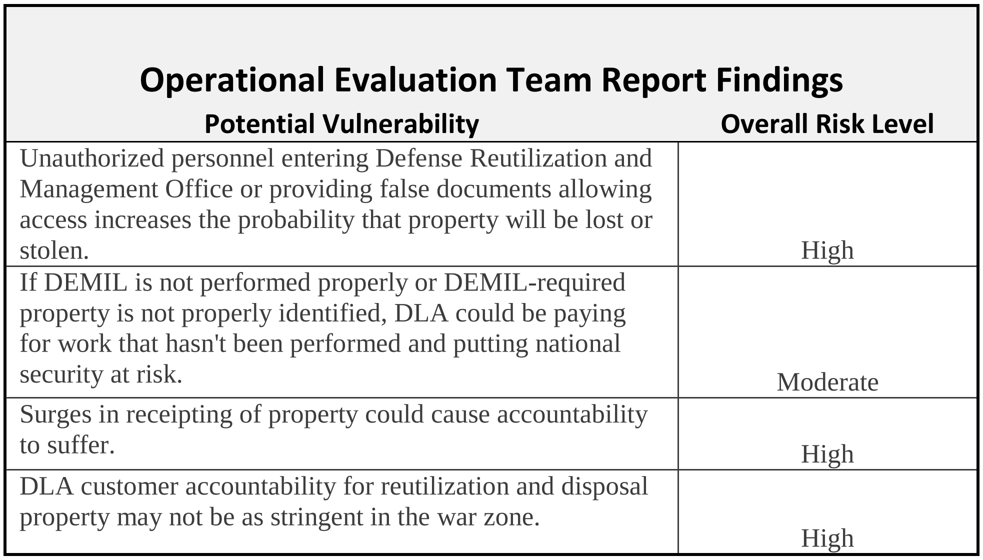
- Difficulties with expeditionary communication during drawdown.

- Uncontrolled dump sites and property accumulation at the FOBs.

- Receipt and processing of serviceable property.

- Limited experienced personnel available to deploy.

The DLA Operational Evaluation Team report, dated April 10, 2010, identified several potential vulnerabilities concerning DLA Disposition Services operations in Afghanistan. The following table outlines the potential vulnerabilities and the corresponding risk level:



Operational Evaluation Team Report Findings

Potential Vulnerability	Overall Risk Level
Unauthorized personnel entering Defense Reutilization and Management Office or providing false documents allowing access increases the probability that property will be lost or stolen.	High
If DEMIL is not performed properly or DEMIL-required property is not properly identified, DLA could be paying for work that hasn't been performed and putting national security at risk.	Moderate
Surges in receipting of property could cause accountability to suffer.	High
DLA customer accountability for reutilization and disposal property may not be as stringent in the war zone.	High

Criteria

In conducting this audit, we relied on these key regulations:

- Department of Defense Directive 4160.21-M, “Defense Materiel Disposition Manual”.
- Department of Defense Directive 4160.28-M, Volume 2, “Department of Defense Manual – Defense Demilitarization: Demilitarization Coding” and Volume 3, “Department of Defense Manual – Defense Demilitarization: Procedural Guidance”.
- DLA Disposition Services 4160.14, “Operating Instructions for Disposition Management”.

Department of Defense Directive 4160.21-M, “Defense Materiel Disposition Manual”, dated August 1997. This manual gives DLA Disposition Services (formally the Defense Reutilization and Marketing Office) the following responsibilities:

- Exercise program management and staff supervision of the Defense Materiel Disposition Program.
- Obtain optimum monetary return to the Government for all property sold.
- Develop programs for surveillance of disposable property and related operations to assure optimum reutilization, proper DEMIL, environmentally sound disposal practices, and performance of functions for which DRMS is responsible under pertinent regulations.
- Prepare solicitations; conduct, execute and administer all sales contracts including the processing of disputes, protests, and claims pertaining to sales and sales contracts.

The Department of Defense Directive on demilitarization coding", dated June 2011:

- Assigns the Secretaries of the Military Department the responsibility for accurate DEMIL codes for every item of DOD personal property they manage.

- Gives DLA the responsibility to provide guidelines for the identification and DEMIL of DOD personal property to prevent its unauthorized use or the potential compromise of US national security; to maintain the DOD DEMIL Coding Management Office (DDCMO) to improve DEMIL code accuracy; and to maintain the Controlled Property Verification Office to support the DDCMO in validating DEMIL codes cited on DOD personal property receipt documents.

Department of Defense Directive 4160.28-M, Volume 3, "Department of Defense Manual – Defense Demilitarization: Procedural Guidance", dated June 2011. This manual assigns DLA the responsibility to provide guidelines for the identification and DEMIL of DOD personal property to prevent its unauthorized use and the potential compromise of U.S. national security. DLA is also responsible to maintain centralized DEMIL centers in order to perform required physical DEMIL. The manual contains information on selecting the method and degree of DEMIL – based on the item in question, performance considerations, and certification and verification requirements for DOD property.

DLA Disposition Services 4160.14, "Operating Instructions for Disposition Management", dated August 2011, states DLA Disposition Services – J9 coordinates with HQ DLA to provide planning services, planning oversight, plans execution, and oversight services to ensure effective and efficient disposal support for Contingencies and Exercises of the Combatant Commander; develops the emergency essential position program; provides implementation of policy of worldwide Emergency Essential (EE)positions; and, provides the administrative support for the disposal remediation team. The instructions provided procedures to support an orderly flow of work, recognizing that property throughput is the key to success. Furthermore, it provided uniform application of DOD/DLA policies.

Operational Structure

At the time of our audit, DLA Disposition Services had three sites operating in Afghanistan. Each site had a site chief to oversee operations, as well as a combination of DLA Disposition Services employees and contract labor support. The following table illustrates the type of personnel assigned to all three sites:

Personnel Breakout		
EDRTs	Contractors	Civilians
31	65	27

In addition, an Area Manager, located in Afghanistan, was responsible for general oversight of all three sites in the country. This oversight included tracking and monitoring Disposition operations and site compliance with existing regulations. DLA Disposition Services deployed EDRT members, who are mostly reservists, to the three Disposition sites in Afghanistan. According to the DLA Disposition Services Contingency Operations training guide, the primary mission of the EDRTS was to support field activity operations and to support disposal operations at FOBs. EDRT functions included educate military customers, survey FOBs to assess scrap disposal requirements, assist with disposal expertise, support disposal operations, and coordinate scrap sales contractor performance and compliance.

From these sites, the EDRT personnel traveled to FOBs throughout Afghanistan to assist units with disposition training and scrap segregation. Each DLA Disposition Services site typically had an Officer-in-Charge (OIC) to oversee the EDRTS assigned to that particular site. An additional OIC located in Kabul had general oversight and management responsibility of the EDRT program.

Contracts

To help accomplish the mission, DLA Disposition Services had several contracts in place to provide labor support, equipment maintenance, and scrap sales throughout Afghanistan.

Labor Support – The CENTCOM Joint Theater Support Contracting Command owned and administered the contract for DLA's labor support in Afghanistan. The service labor contract provided DLA with 65 personnel at all three sites, to include management oversight. Types of labor provided to DLA included torch cutters, material handling equipment operators, laborers, customer service clerks, and administrative assistants. The contracting officer was located in Afghanistan, and one of the DLA Disposition Services site chiefs held the responsibility as the contracting officer's representative (COR) for all three sites.

Equipment Maintenance – DLA Disposition Services had one contract in place to provide equipment maintenance support to all three sites in Afghanistan. DLA awarded this contract in February 2012. The contractor will provide scheduled preventative equipment maintenance to the sites approximately every three months, based upon material handling equipment identified by DLA. The contractor will also provide unscheduled maintenance and repair services within three days after responding to the contracting officer's request for repair. Each site chief was designated as the COR for the contract line item associated with their site.

Scrap Sales – DLA Disposition Services awarded nine scrap sales contracts to different contractors in Afghanistan. The scrap sales contractors covered different areas of Afghanistan based on their geographic location in the country. The contracting officer was located at DLA Disposition Services Headquarters in Battle Creek, Michigan. DLA sold the scrap to the contractors at a fixed price per pound to remove metallic and non-metallic scrap from sites.

Demilitarization Coding

All DOD personal property acquired for military use is evaluated for DEMIL requirements, and a DEMIL code is assigned to each item to identify the degree of DEMIL required. The DEMIL code for National Stock Number (NSN) items is posted to the Federal Logistics Information System (FLIS). DEMIL codes for non-NSN items can be found in acquisition program-managed inventory management systems. According to DOD 4160.28-M, Volume 2, the Controlled Property Verification Office (CPVO) supports the DDCMO to improve and validate DEMIL coding of items turned in to DLA Disposition Services by military units. CPVO support includes challenging DEMIL codes that may be incorrect. The CVPO accomplishes this by actively reviewing the DEMIL codes for items received onto the DLA Disposition Services Automated Information System (DAISY) accountable record by NSN.

In DAISY, XR1, XR2, and XR3A are transaction codes which represent the receipt of usable property, the receipt of scrap, and the downgrade receipt to scrap, respectively. In addition to the DEMIL code, these are the main codes assigned to items received at the DLA Disposition Services sites in Afghanistan.

RESULTS, RECOMMENDATIONS, AND CONCLUSIONS

RESULTS AND RECOMMENDATIONS

DLA Disposition Services generally had sufficient policies and controls in place to accomplish the mission. However, DLA Disposition Services should strengthen policies and controls related to the theater-specific missions and challenges to increase assurance of mission success throughout drawdown operations.

The three DLA Disposition Services sites typically conducted operations concerning property receipt, demilitarization, reutilization, and backlog processing in accordance with existing DOD and DLA policies. We found that all three sites were laid out to facilitate the receipt of property, and personnel at two of the three sites processed receipts appropriately. We observed all three sites performing the physical demilitarization of items in accordance with applicable guidance and two of the three sites only allowed authorized personnel to reutilize property. Although we noted one site that had an excessive amount of spent brass without proper inert certifications, none of the sites allowed daily receipt backlog to occur. Personnel at the site with excessive spent brass developed and implemented a process to certify and dispose of the items during our audit.

We also reviewed the utilization and distribution of resources, to include the EDRT, support contracts, and equipment. DLA Disposition Services recently established an equipment maintenance contract to address equipment challenges unique to Afghanistan. EDRTs deployed in Afghanistan frequently visited FOBs, as intended by the program.

However, DLA can strengthen policies and controls related to the theater-specific missions and challenges to improve drawdown operations. Specifically, we identified weaknesses in the controls related to scrap operations, DEMIL records and coding, contracts, and the EDRT mission.

Scrap Operations

At two sites, DLA Disposition Services did not inspect contractor vehicles or monitor scrap truck drivers on site. Additionally, at one site DLA Disposition Services did not weigh-in trucks prior to loading scrap. Scales were not inspected and calibrated at all three sites in Afghanistan. This occurred because DLA Disposition Services personnel continued the process that previous personnel had followed rather than developing theater-specific procedures. As a result, contractors may not have paid for all scrap material they received.

DOD 4160.21-M states DLA Disposition Services personnel or representatives should:

- Inspect all sales property when it is delivered or shipped to purchasers in order to prevent error, fraud, or theft.

- Weigh property sold at the time of delivery to the purchaser.

- Ensure the weight scales are inspected on a frequency and not less than annually.

Additionally, DRMS-I 4160.14 states DLA Disposition Services personnel or representatives should:

- Inspect vehicles entering the field activity for removing property by weight for extraneous cargo or suspicious items that could be used to inflate their weight.

- Utilize activity employees and/or closed circuit television to escort/monitor visitors to preclude pilferage or improper handling of property.

- Re-inspect vehicles departing the field activity to ensure that all cargo and personnel in the vehicle at the time of weigh in are present on weigh out and perform a visual inspection of loaded material to prevent unauthorized removal of property/verify removal authority.

We observed 26 scrap sales transactions at the three Disposition sites in Afghanistan and noted the following:

Scrap Sales Observations			
Discrepancy	**Site 1**	**Site 2**	**Site 3**
No vehicle inspection upon entry	7 of 7	9 of 9	10 of 10
No weigh-in upon entry	0 of 7	0 of 9	10 of 10
No driver escort/monitoring	2 of 7	9 of 9	5 of 10
No exit inspection	7 of 7	7 of 9	10 of 10

None of the 26 selected transactions had entrance inspections, and only 2 of the 26 transactions had exit inspections. We determined that DLA Disposition Services personnel did not inspect vehicles entering or exiting the scrap yards because each vehicle was inspected at the installation access control point. However, installation access control procedures were designed to protect personnel and ensure only authorized personnel entered the base without weapons or explosive devices. Installation access control procedures were not intended to prevent unauthorized property removals. The installation access control point inspections did not mitigate the fraud potential and therefore, should not have precluded DLA personnel from conducting vehicle inspections.

The three DLA Disposition Services sites we audited did not monitor or escort contractor personnel while they were in the scrap yard for 16 of the 26 reviewed transactions. We observed:

- One site relied on installation-contracted escorts to monitor the drivers. While these escorts remained at the site during the scrap loading process, they did not provide oversight of the drivers in the scrap yard.

- Two sites relied on either DLA-contracted employees or a DLA employee to monitor the entire scrap removal process for multiple vehicle drivers.

Inconsistent monitoring of contractor personnel while in the scrap yard occurred because current DLA Disposition Services personnel continued the process that previous personnel had followed rather than developing theater-specific procedures. As a result of the inconsistent procedures, at one site, we witnessed a truck driver move freely among the segregated scrap piles in the yard and remove an item.

One site did not weigh-in vehicles prior to loading scrap. Instead, DLA Disposition Services personnel completed scrap sales documentation by using the initial weight of the vehicle (the weight of the vehicle the first time it received scrap) and the actual weight upon departure. We weighed four of the vehicles prior to loading to determine if there was a substantive difference in weights and found that all four vehicles weighed less than the documented weight by about 2,060 kilograms or 3.7 percent. When projected over the FY 12 second quarter sales of 5.6M kilogram of scrap, DLA Disposition Services did not bill for 204,140 kilograms. This occurred because DLA Disposition Services personnel continued the process that was in place and passed down as a theater-specific practice when personnel deployed to the site. As a result of this improper practice, DLA did not bill the contractor for the entire amount of scrap removed and subsequently did not collect monies owed from the contractor.

All three DLA Disposition Services sites in Afghanistan had scales capable of weighing scrap contractor vehicles and although the scales were generally used, DLA had not completed the annual inspections required by DOD 4160.21-M and DRMS-I 4160.14. We could not determine when the last inspection and calibration occurred at all sites due to a lack of documentation, nor did the site chiefs know. This occurred because of a lack of theater-specific policy and oversight and because of the short duration of personnel rotation into the sites. As a result, DLA may not be accurately billing the contractor for scrap sales.

Recommendation 1 (DLA Disposition Services)
Develop theater-specific guidance addressing critical operational areas in order to prevent fraud, waste, and abuse given the operating environment. Specifically, the guidance should address inspection and weighing of vehicles entering the scrap yard and monitoring of contractor employees in the scrap yard.

Management Comments
Concur. Disposition Services stated all employees were briefed as of October 7, 2012 on the proper handling of scrap contractors while on a DLA site. As a result, scrap contractors are required to either 1) remain in their vehicle, or 2) remain in a defined location while awaiting loading of scrap. Disposition Services does not think additional theater-specific guidance is needed. To ensure compliance, the Site Chief and Area Manager periodically review the entry, loading and release of scrap trucks to ensure proper procedures are followed for inspecting and releasing scrap contractor trucks.

OIG Analysis of Management Comments
Management Comments were responsive.

Recommendation 2 (DLA Disposition Services)
Ensure that site chiefs obtain the required annual inspections and calibrations for all scales or a waiver.

Management Comments
Concur. Disposition Services submitted a Statement of Work to obtain a contract for the annual inspection for scales at applicable sites in Afghanistan, with the expectation of having a contract in place no later than 13 January, 2013.

OIG Analysis of Management Comments

Management Comments were responsive.

Demilitarization Records

Although DLA Disposition Services performed the physical DEMIL of items in accordance with applicable guidelines, site personnel did not always follow required DEMIL certification and documentation procedures. These discrepancies occurred because personnel were not always sure of their job responsibilities and because of unclear theater-specific guidance. Therefore, DLA may not have records to support the proper handling of sensitive property.

We observed 37 DEMIL transactions and found that DLA Disposition personnel performed the physical DEMIL procedures in accordance with specific DLA guidance. Additionally we noted site personnel utilized DAISY or Web Federal Logistics Information System (WEBFLIS) to identify items requiring DEMIL and stored them appropriately to protect against theft in accordance with DRMS-I 4160.14. However, we noted one type of discrepancy during our DEMIL observations.

Certification. DRMS-I 4160.14 defines a DEMIL certifier as a technically qualified Government representative who actually performed or supervised the required DEMIL. We found 11 DEMIL certificates that were completed by a certifier without either performing or supervising the physical DEMIL process. This occurred because DLA Disposition Services personnel were not required to complete specific training, such as DEMIL, prior to deployment. As a result of DEMIL certifiers not sufficiently performing their role, controls were not in place to ensure DEMIL was performed properly by contract personnel.

We also tested 76 turn-in transactions at the three sites that required DEMIL certifications and identified two types of discrepancies in the DEMIL documentation.

Training. DRMS-I 4160.14 requires certifiers and verifiers to complete classroom training every three years and a complete a refresher course every year not attending classroom training. DLA Disposition Services had eleven personnel located at the three sites that certified or verified DEMIL transactions between January 1, 2012 and March 30, 2012. Of those eleven personnel, two employees did not meet the annual DEMIL training requirements. Although one employee had redeployed at the time of our review, the remaining employee immediately completed the annual training requirement during our site visit. This occurred because personnel deployed to contingency sites may serve in a variety of roles outside of their normal duties with DLA Disposition Services, to include DEMIL certifier and verifier and are therefore unaware of the requirements.

Document Retention. One transaction requiring DEMIL was no longer on the site's accountable record and the DEMIL certificate was not available to show the item had been demilitarized. This occurred because the site certified and verified multiple DEMIL items on one single inventory list, instead of preparing individual DEMIL certificates. As a result, site personnel could not show that an item with offensive or defensive military capabilities was processed appropriately prior to being released to a scrap contractor for removal. Although DLA guidance allows multiple DEMIL certifications, a better practice would be to certify and verify DEMIL transactions individually and upload all DEMIL certificates in to the electronic records database.

Recommendation 3 (DLA Disposition Services)
Identify training for all pre-deployed personnel to receive in order to ensure employees understand most position requirements and to create a cross-leveled workforce.

Management Comments
Concur. Disposition Services stated training requirements are currently listed in the training plans of all employees deployed in the Civilian Expeditionary Workforce (CEW); and deployment training requirements for all CEW employees are listed in the DLA Learning Management System (LMS). Additionally, a "boot camp" of hands on deployment training for CEW employees is in development. The first training date is scheduled for May 11-24, 2013. This beneficial training will include all duties CEW employees will encounter once they arrive on site, ready to begin work.

OIG Analysis of Management Comments
Management Comments were responsive.

Recommendation 4 (DLA Disposition Services)
Develop a database to track certification and verification records of items with offensive or defensive military capabilities and requiring demilitarization actions.

Management Comments
Concur. Disposition Services stated that beginning on November 30, 2012, the local Site Chief will verify the identified process in accordance with the quarterly Self-Assessment in the Compliance Management System (CAMS) to ensure DEMIL documents are appropriately filed. The OIG agreed that adding a database would be cumbersome and not likely improve the ability of the Afghanistan site or DLA Disposition Services to maintain required documents.

OIG Analysis of Management Comments
Management Comments were responsive.

Demilitarization Coding

We identified an inconsistency between the DEMIL and integrity codes, both of which play a part in determining how to DEMIL property. We discovered this inconsistency when we identified two helmets that did not appear to be processed to remove defensive capabilities and were ready to be loaded in to a scrap contractor vehicle. When we brought this to their attention, the site immediately shredded the helmets to ensure complete mutilation. Additionally, the DEMIL code for the helmets has been changed from DEMIL A (no DEMIL processing was required prior to disposition) to DEMIL D (total destruction of item and components to prevent restoration or repair to a usable condition).

The helmets were initially coded as DEMIL A in both WEBFLIS and Federal Logistics (FEDLOG), which indicates no DEMIL processing was required prior to disposition. WEBFLIS also showed that the helmets were initially given a DEMIL integrity code of 4, which indicates that a DEMIL code could not be validated due to insufficient technical data. DLA Disposition Services personnel stated that items with an integrity code of 4 are generally given a DEMIL Code A until further information is available to assign the appropriate DEMIL code.

The inconsistency between the DEMIL and integrity codes occurred because the Controlled Property Verification Office only reviewed data for items coded in the accountability system as a "receipt of usable property" (XR1) transaction, but didn't review the items coded as "downgraded to scrap" (XR3). Additionally, the CPVO did not have a procedure in place review items with an integrity code of 4 to determine whether there is sufficient technical data had been received so that the correct DEMIL code could be assigned to the item.

As a result, DLA Disposition Services might have inadvertently released usable military equipment to an Afghan scrap contractor that could be used against U.S. forces.

Recommendation 5 (DLA Disposition Services)
Establish procedures in the Controlled Property Verification Office to periodically perform a review of items with integrity code 4, as well as "downgrade to scrap" transactions, to determine if DEMIL codes are accurate.

Management Comments
Concur. Disposition Services maintains accountability of all demil-required property. A new, enhanced process added on April 30, 2012. Specifically, the Controlled Property Verification Office (CPVO) reviews weekly all National Stock Numbers (NSNs) received into the DLA Disposition Services inventory for DEMIL code accuracy. The CPVO reviews NSNs with integrity code 4; and, the DEMIL Verification at Receipt (DVR) process includes all DEMIL B and Q NSNs with integrity code 4. Downgrades to scrap transactions are reviewed for DEMIL code accuracy at the receipt stage as part of the review. At field locations, if an unusual item is noticed in a scrap pile at a particular site, it is pulled out immediately as part of the management of the scrap pile process.

OIG Analysis of Management Comments
Management Comments were responsive.

Contract Administration

DLA Disposition Services needs to improve the administration of the contracts for labor support, scrap sales, and material handling equipment. Also, DLA Disposition Services needs to address issues with contractor training and oversight, contract requirements, and performance evaluation.

Labor Contract. We evaluated the turn-in process for 75 property receipts at the three sites. Specifically we evaluated whether site personnel:

- Reviewed the Disposal Turn-In Document (DTID) for completeness, proper signatures, and correct item quantity/nomenclature.
- Ensured the serviceable property statement was included on the DTID, when applicable.
- Stored property appropriately and correctly annotated its location on the DTID.

- Ensured the customer provided all necessary statements and certifications, such as inert certificates, at the time of turn-in.

- Entered property turn-in information in to the accountable system accurately and completely, based on the DTID.

Generally, contract personnel received property (turn-ins) in accordance with DOD 4160.21-M and DRMS-I 4160.14. We also observed personnel assist the customer with fulfilling turn-in requirements on-site, such as researching property data in WEBFLIS and FEDLOG, providing blank certification forms at the site, and providing instructions for document completion. One site provided customers with a Form 917 if the site could not accept any property. The purpose of the form was to clearly explain to the customer why an item was rejected, and what was needed to turn it in. Although the property was not received by the site and formally rejected, giving the customer the Form 917 may be a best practice to improve customer satisfaction.

Although the receipt process was generally in place and operating, DLA Disposition Services contract labor personnel did not always follow existing DOD and DLA guidance for site operations. For example, we observed the following:

- Serviceable items were informally rejected contrary to new DLA SOP.

- Turn-in documentation wasn't verified – we identified one item DLA would have taken accountability for (valued at about $19,800) without physically receiving it; and a physical receipt of two items (valued at about $114,000) while only accounting for one item. The site corrected these discrepancies when we brought them to the chief's attention.

- Secured cage was left open and unattended.

- Customers were allowed to leave with items from the yard without properly following the reutilization process.

These conditions occurred for two reasons. First, the Contracting Officer, located at the Bagram Regional Contracting Center, could not determine which contractors were trained or provide any records of contractor training. Moreover, the Contracting Officer did not have the new DLA Standard Operating Procedure for processing serviceable goods to forward to responsible contract personnel for implementation. Additionally, the contractor did not have any internal standard operating procedures in place at the site for employees' reference. The lack of a formalized training program and training records created limited assurance that personnel involved in daily site operations fully understood current policies.

Secondly, at the time of our audit, there was only one Contracting Officer's Representative (COR) appointed to provide contractual oversight of all three DLA Disposition Services sites in Afghanistan. There was also a period of about three months where no appointed COR was in place to certify invoices, verify contractor job performance, or provide direction to the contractor. DLA did not provide monthly contractor performance evaluations to the contracting officer.

Recommendation 6 (DLA Disposition Services)
Assign each site chief Contracting Officer's Representative responsibilities for the labor contract and provide monthly evaluations and updated policies to the Contracting Officer.

Management Comments
Concur. Disposition Services changed the COR oversight process on (or about) May 30, 2012 as a result of the finding leading to this recommendation. Each Site Chief obtains the defined Defense Acquisition University (DAU) required training before entering Afghanistan. Once on site, the incoming Site Chief attends the required training (as assigned by the Contracting Officer) that can only be obtained in country. Now, each Site Chief is assigned as Contracting Officer Representative (COR) for the labor contract in effect for their site. Each COR provides monthly evaluations to the Contracting Officer. The contracting office for the DLA Disposition Services labor contract in Afghanistan is the Army Regional Contracting Office in Bagram. This follow-on Army contract will soon be replaced by a new DLA Disposition Services contract (projected to be in place by July 2013) and will include these requirements: 1) A COR must be assigned at each site; and, 2) the CORs will be required to provide monthly status reports.

OIG Analysis of Management Comments
Management Comments were responsive.

Recommendation 7 (DLA Disposition Services)
Conduct periodic refresher training with the contract personnel on site to ensure new and existing DOD and DLA policies are understood and followed over the course of operations.

Management Comments
Concur. To address this concern, each site implemented a "receiver" (contract employee) training on (or about) October 7, 2012. This class is held bi-weekly to discuss issues found during the previous weeks, as well as to instruct the contract employees on any new procedures or policies DLA implements.

OIG Analysis of Management Comments
Management Comments were responsive.

Scrap Sales. DLA Disposition Services sites employed different methods of issuing access request memorandums to the scrap contractors.

- One site provided all signed access memorandum to the first contractor coming to the site that month, with the intent they would deliver the memorandums to the contractor's office.

- One site provided the access memorandums directly to the scrap contractor's program manager.

The different methods of providing the access memorandums to the scrap contractor increased the force protection risk assumed by DLA. This occurred because the DLA scrap contracting officer allowed the site chiefs to decide how to provide access support to the scrap contractors. While each installation could have different access control procedures, standardization of this process would reduce force protection risks and ensure that only personnel designated by the contracting officer receive the access request memorandums.

Recommendation 8 (DLA Disposition Services)
Establish and implement written procedures for scrap contractor-required support concerning installation access. Procedures should identify who is an authorized recipient of DLA-signed memorandums, and acceptable methods to provide the memorandums to the contractor.

Management Comments
Concur. In order to standardize the process, all sites will now follow the same procedure, as of October 7, 2012. The access letter is provided to the company's authorized representative either in person; or, scanned and e-mailed to the company ahead of the date of required access needed. DLA letters of access apply directly to a driver's Teskara (unique personal identification) and are for a defined period of performance as referenced in the letter. Each site has a file of each letter of access approved by the installation. The access procedures followed by DLA will be uniform in procedure. DLA will coordinate with each location's base personnel to insure compliance with base requirements while assuring effective but secure access for its contractors.

OIG Analysis of Management Comments
Management Comments were responsive.

Equipment. While DLA Disposition Services recently established a material handling equipment maintenance contract for the three sites in Afghanistan, responsible personnel needed to track additional performance metrics. The intent of the contract was to improve equipment availability since DLA Disposition Services identified equipment maintenance as a challenge in Afghanistan. The contract listed all of the material handling equipment that the contractor was responsible for maintaining. The three disposition sites tracked the status of their material handling equipment on a weekly basis, and provided the mission-capable percentage rate to leadership. However, DLA Disposition Services personnel could not determine how long individual pieces of equipment were inoperable. This occurred because the duration that each piece of equipment was inoperable was not tracked. However, this type of information would demonstrate the efficiency and effectiveness of the contractor. Additionally, tracking the duration of inoperable equipment could help site chiefs prioritize the contractor's work, demonstrate serious problems with equipment downtime to leadership, and provide continuity of operations for site chief turnover.

Recommendation 9 (DLA Disposition Services)
Develop and implement performance metrics to track the length of time Material Handling Equipment is out of service, to ensure the contractor performs according to contract requirements.

Management Comments
Concur. Beginning in December of 2011, equipment readiness became an item of discussion in a weekly DLA Disposition Services maintenance teleconference. This meeting includes site chiefs, on-site maintainers, DSD-Central staff, a contracting representative, DLA Installation Support representatives, and the appropriate staff from DLA Disposition Services**.** The DSD-Central Equipment Readiness/Remediation Team (ERT) has been tracking equipment down time since approximately 15

January 2012. Tracking includes: a) when the equipment is first reported non-operational, b) what is at fault with the equipment; c) the estimated repair completion date, d) order status; and, e) other pertinent information. Disposition Services stated they are tracking contractor performance to ensure equipment down time is minimized and that the contractor, Relyant, is accountable for timely repairs.

OIG Analysis of Management Comments

Management Comments were responsive.

EDRT Mission

DLA Disposition Services needs to improve the administration of EDRT program through standardization of training and communication in order to ensure optimal utilization of valuable resources.

Utilization. The EDRT program in Afghanistan can be strengthened and improved with the implementation of standardized procedures and training. The EDRT mission is structured to provide training and to facilitate scrap removal support to units located at FOBs, and to assist with operations at the Disposition sites in Afghanistan. DLA Disposition Services typically tracked the amount of scrap that EDRTS assisted in removal of from the FOBs. All three sites implemented a utilization tracking process to have better visibility of personnel. However, there were inconsistencies in level of details and the type of information tracked and maintained by the sites.

For example, all three sites used different reports when communicating between the site and the EDRT. The extent of EDRT assistance with the identification, separation, and shipping preparation of DEMIL-required items was not fully captured by any reports submitted to EDRT leadership. Some reports contained details on DEMIL-required items and the number of containers to ship back to a DLA Disposition Services site, but this information was not always reported or shared with the site chiefs for workload planning purposes. As a result, it was difficult to determine the effectiveness of EDRT personnel in their assistance with ensuring units properly processed DEMIL-required property.

The emphasis seems to be on the pounds of scrap removed from the site because only scrap removal is actively tracked at all three sites. Due to the lack of specificity in different reports and the lack of tracking by the OICs, we couldn’t determine the extent of EDRT utilization, aside from which FOB they visited and when. Additionally, one site could not provide any reports between 6 January and 10 April 2012, although EDRTS conducted visits to FOBs during this timeframe

Each site had different methods in place to determine and to plan EDRT travel to FOBs. One site relied mainly on emails from units requesting assistance, and the other sites proactively identified FOB closure dates to determine where disposition assistance may be needed, together with customer requests for support. One site had EDRTS actively involved with mobile military redistribution teams; however, it was not clear whether the expectation was for all sites to participate with these types of teams. The reactive approach to planning site visits may not have resulted in maximized utilization of EDRTS. For example, the sites that proactively planned FOB visits usually had higher EDRT utilization rates and less downtime at their duty stations.

EDRTs can also improve communications with the Mayor Cell/Garrison Command and EDRT involvement at the duty station. One of the lessons learned from Iraq was to partner with Mayor

Cells/Garrison Commands for EDRT missions. In most instances, the Mayor Cell/Command was the primary starting point of the mission, in terms of helping to coordinate site visits. However, EDRTs did not provide Mayor Cell/Garrison Commands with any type of after action reports to identify issues or provide general feedback on the mission. Some of the EDRT reports noted issues with the FOBs, which should be communicated to the FOB leadership in an effort to improve operations. Additionally, EDRTs we interviewed indicated a concern with the lack of involvement by the right level of leadership at the FOBs throughout the training and removal process. Since EDRTs may visit a site multiple times, it would be beneficial to keep the Mayor Cell/Garrison Commands involved in the entire realm of operations, from start to finish.

We could not determine the level of the EDRT support provided to the Disposition sites when EDRTs were not at FOBs. We observed some EDRTs assisting with scrap contractor escorts at one site, yet at another site, we observed no EDRT involvement with site operations. From the utilization reports, there was a varying level of support provided to the sites by the EDRTs when they were not visiting FOBs. For example, one EDRT remained at the Disposition site for 24 days, and only reported 6 days of site assistance. There were other instances noted where EDRTS did not assist the site, based on the utilization reports.

Training. The sites employed varying levels and types of EDRT training during deployment. EDRT training should be consistently applied across the sites to ensure standardization of operations in the field and that all personnel have the same skillset and knowledge base to perform the mission. As an example, one site assessed the EDRT's knowledge of disposition operations at the beginning of deployment, and implemented on-the-job training in-between FOB visits. Another site did not have any on-going training in place or preliminary knowledge assessments. As a result, EDRTS may not be fully aware of policies specific to Afghanistan, or any changes in the mission, such as the new serviceable items SOP.

Communication. EDRT personnel established a Yahoo group e-mail account, in order to communicate while deployed to the sites and to receive assistance requests from FOBs. Communication between the EDRTs and the Disposition Sites often included details on the scrap removal process, such as when scrap trucks were expected at the FOB and other operational issues at the site. However, there may be operational security concerns with the utilization of a non-government e-mail account to share information.

These conditions occurred due to a lack of a standardized process to track EDRT utilization, to include formalized guidance specific to the EDRT mission in Afghanistan. The development and implementation of EDRT policy and guidance for Afghanistan can help ensure appropriate mission requirements are followed and establish metrics to measure success.

Recommendation 10 (DLA Disposition Services)
Develop and implement standard operating procedures for the EDRT program, to include program expectations, metrics to measure success, and examples of standardized reports and training materials for the sites.

Management Comments

Concur. Currently, EDRT teams across the Combined Joint Operations Area (CJOA) use Standard Operating Procedures (SOPs) and training programs that were aligned for the entire CJOA, not solely for Afghanistan deployment. To remedy this, DSD-Central is staffing a separate draft CJOA-wide EDRT SOP. This new, revised SOP will place focus on Afghanistan-centric roles and responsibilities, command and control, missions, operational checklists, reporting requirements, and measures of performance and effectiveness. The DSD Central will take these steps toward completion:
15 November 2012: Vet final draft EDRT SOP across the DLA Disposition Services team:
15 December 2012: Complete the coordinated EDRT SOP; and,
15 January 2013: Release final EDRT SOP to workforce (and provide a copy to the OIG).

OIG Analysis of Management Comments

Management Comments were responsive.

Recommendation 11 (DLA Disposition Services)

Update pre-deployment EDRT training to focus on current operations in Afghanistan, also incorporating EDRT standard operating procedure guidance.

Management Comments

Concur. Afghanistan specific training was recently added to the EDRT pre-deployment training regimen as a result of this finding. DLA Disposition Services believes it is important that the EDRT training program continue to involve a well-rounded curriculum so EDRTs have the skillsets they need to operate in any environment (including and beyond Afghanistan). We are striving to train well-rounded, technically and tactically agile EDRTs, for both current and future operating environments. Also, as indicated in our response to Recommendation 10, the current EDRT training regimen is for the CJOA, not only Afghanistan. The new EDRT SOP will help to focus EDRT personnel, once they arrive on site, to work in Afghanistan. Pre-deployment training modifications are in the progress; and, (beginning January 15, 2013), the EDRT annual training program will be modified to include Afghanistan-specific topics.

OIG Analysis of Management Comments

Management Comments were responsive.

Recommendation 12 (DLA Disposition Services)

Establish appropriate communication methods between EDRTS and the sites, which minimizes operational security issues from the transmittal of potentially sensitive information.

Management Comments

Concur. As a result of this finding, standardized procedures were put into place on June 15, 2012 to ensure EDRTs operating in the AOR do not use open, non-encrypted email. EDRTs are now required to employ service “For Official Use Only” (FOUO) email platforms such as Defense Knowledge Online or Army Knowledge Online. EDRT training and the new, draft EDRT SOP both include communication security protocols and guidance concerning OPSEC concerns. EDRT personnel are equipped with satellite telephones to ensure they have continued voice communications even when there is no cell coverage.

OIG Analysis of Management Comments

Management Comments were responsive.

CONCLUSIONS

DLA Disposition Services generally had sufficient policies and controls in place to accomplish the mission. The three DLA Disposition Services sites conducted operations concerning property receipt, actual demilitarization of items, reutilization, and backlog processing typically in accordance with existing DOD and DLA policies. DLA Disposition Services recently established an equipment maintenance contract to address equipment challenges unique to Afghanistan. EDRTS deployed in Afghanistan frequently visited FOBs, as intended by the program.

However, policies and controls related to the theater-specific mission and challenges can be strengthened and improved, particularly to increase assurance of mission success throughout drawdown operations. Our audit yielded weaknesses in the controls related to aspects of scrap operations, DEMIL records and coding, contracts, and the EDRT mission. Additionally, personnel occasionally deviated from the overarching DOD and DLA policies governing operations due to established practices in the theater environment. The deviation from overarching DOD and DLA policy and the propensity for sites to conduct operations independently resulted largely from a lack of theater-specific guidance and no established training requirements for all personnel involved in contingency operations. As a result, DLA Disposition Services may not be able to provide optimal support to the Warfighter and may not be best postured to handle future drawdown support requirements.

The development and implementation of theater-specific guidance would give DLA Disposition Services the opportunity to emphasize important aspects of operations occurring in Afghanistan, and would help ensure processes are standardized. This would allow for easier monitoring by leadership and greater accountability by DLA employees and contractors alike.

SUMMARY OF RECOMMENDATIONS

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
1	Develop theater-specific guidance addressing critical operational areas in order to prevent fraud, waste, and abuse given the operating environment. Specifically, the guidance should address inspection and weighing of vehicles entering the scrap yard and monitoring of contractor employees in the scrap yard.	Director, DLA Disposition Services	Closed	October 7, 2012
2	Ensure that site chiefs obtain the required annual inspections and calibrations for all scales or a waiver.	Director, DLA Disposition Services	Open	January 13, 2013
3	Identify training for all pre-deployed personnel to receive in order to ensure employees understand most position requirements and to create a cross-leveled workforce.	Director, DLA Disposition Services	Open	May 11-24, 2013
4	Develop a database to track certification and verification records of items with offensive or defensive military capabilities and requiring demilitarization actions.	Director, DLA Disposition Services	Closed	November 30, 2012
5	Establish procedures in the Controlled Property Verification Office to periodically perform a review of items with integrity code 4, as well as “downgrade to scrap” transactions, to determine if DEMIL codes are accurate.	Director, DLA Disposition Services	Closed	April 30, 2012
6	Assign each site chief Contracting Officer’s Representative responsibilities for the labor contract and provide monthly evaluations and updated policies to the Contracting Officer.	Director, DLA Disposition Services	Closed	May 30, 2012

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
7	Conduct periodic refresher training with the contract personnel on site to ensure new and existing DOD and DLA policies are understood and followed over the course of operations.	Director, DLA Disposition Services	Closed	October 7, 2012
8	Establish and implement written procedures for scrap contractor-required support concerning installation access. Procedures should identify who is an authorized recipient of DLA-signed memorandums, and acceptable methods to provide the memorandums to the contractor.	Director, DLA Disposition Services	Closed	October 7, 2012
9	Develop and implement performance metrics to track the length of time Material Handling Equipment is out of service, to ensure the contractor performs according to contract requirements.	Director, DLA Disposition Services	Closed	June 15, 2012
10	Develop and implement standard operating procedures for the EDRT program, to include program expectations, metrics to measure success, and examples of standardized reports and training materials for the sites.	Director, DLA Disposition Services	Open	January 15, 2013
11	Update pre-deployment EDRT training to focus on current operations in Afghanistan, also incorporating EDRT standard operating procedure guidance.	Director, DLA Disposition Services	Open	January 15, 2013
12	Establish appropriate communication methods between EDRTS and the sites, which minimizes operational security issues from the transmittal of potentially sensitive information.	Director, DLA Disposition Services	Closed	June 15, 2012

APPENDIX B

ABBREVIATIONS USED

CPVO – Controlled Property Verification Office

COR – Contracting Officer’s Representative

DAISY - Disposition Services Automated Information System

DDCMO – DoD Demilitarization Coding Management System

DEMIL – Demilitarization

DTID – Disposal Turn-in Document

EDRT – Expeditionary Disposal Remediation Team

FEDLOG – Federal Logistics

FLIS – Federal Logistics Information System

FOB – Forward Operating Base

MIDAS - Management Information Distribution and Access System

NSN – National Stock Number

WEBFLIS – Web Federal Logistics Information System

APPENDIX C

OTHER OBSERVATIONS

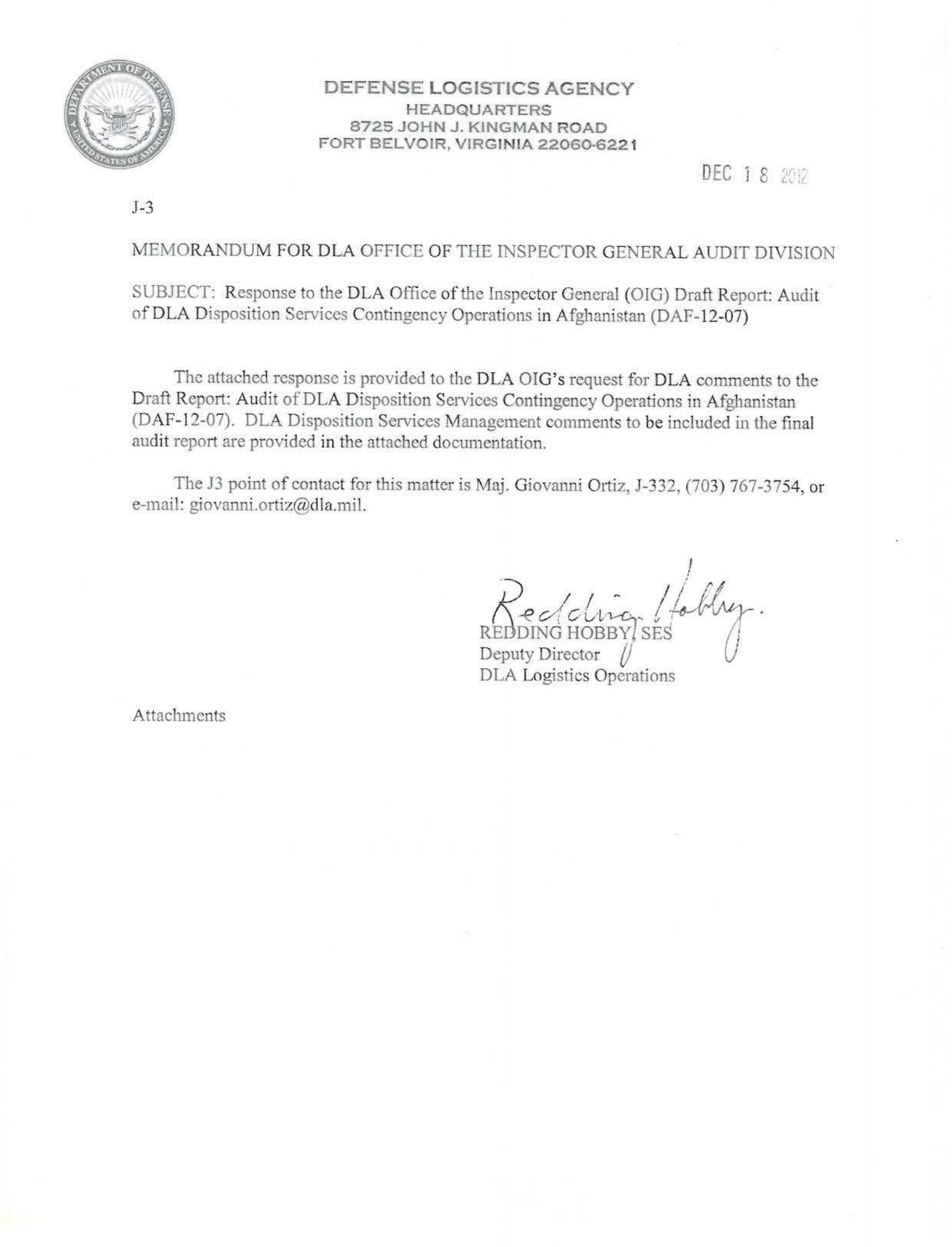
During our site visits, we observed potentially unsafe scrap loading procedures occur at some of the DLA Disposition Services sites in Afghanistan. The scrap contract truck drivers actively participated in the loading of the scrap trucks, mainly by standing in the bed of the scrap truck as a DLA contract employee operating a forklift loaded the truck. We are concerned about the possibility of an accident occurring at a DLA Disposition Services site resulting from the scrap contract driver's participation in the scrap truck loading process.

Furthermore, the scrap sales contract, under which these trucks were loaded, did not require the contractor to obtain and carry Defense Base Act insurance, as the two DLA service contractors for labor support and equipment maintenance were required to have.

Although we have no recommendation for this situation, DLA leadership may want to ensure that the U.S. Government would not be liable should an accident occur at DLA Disposition Services sites in Afghanistan.

APPENDIX D

MANAGEMENT COMMENTS



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

DEC 18 2012

J-3

MEMORANDUM FOR DLA OFFICE OF THE INSPECTOR GENERAL AUDIT DIVISION

SUBJECT: Response to the DLA Office of the Inspector General (OIG) Draft Report: Audit of DLA Disposition Services Contingency Operations in Afghanistan (DAF-12-07)

The attached response is provided to the DLA OIG's request for DLA comments to the Draft Report: Audit of DLA Disposition Services Contingency Operations in Afghanistan (DAF-12-07). DLA Disposition Services Management comments to be included in the final audit report are provided in the attached documentation.

The J3 point of contact for this matter is Maj. Giovanni Ortiz, J-332, (703) 767-3754, or e-mail: giovanni.ortiz@dla.mil.

Redding Hobby.

REDDING HOBBY, SES
Deputy Director
DLA Logistics Operations

Attachments

DLA Disposition Services Response
to DLA Office of Inspector General Draft Report dated October 15, 2012
Audit of DLA Disposition Services Contingency Operations in Afghanistan

Proposed Final Response December 7, 2012

Scrap Operations

Recommendation 1: Develop theatre-specific guidance addressing critical operations in order to prevent fraud, waste and abuse given the operating environment. Specifically, the guidance should address inspection and weighing of vehicles entering the scrap yard and monitoring of contractor employees in the scrap yard.

Response: Concur

If this process is not followed, it means personnel are not following proper procedures, as our policy requires all trucks be weighed. A theatre-specific reminder was needed since the DLA OIG team observed no inspection of contractor vehicles or monitoring of scrap drivers at two sites. To address this, all employees were briefed on (or about) **October 7, 2012** on proper handling of scrap contractors while on a DLA site. To ensure adherence to this procedure; and, to correct this finding, scrap contractors are now required to either:

1) remain in their vehicle, or
2) remain in a defined location while awaiting loading of scrap.

To ensure compliance, the Site Chief and Area Manager periodically review the entry, loading and release of scrap trucks to further guarantee proper procedures are followed for inspecting and releasing scrap contractor trucks.

The sections in the DRMS 14160.14 related to inspecting and weighing scrap are:

C2.15.5.1.2. **Weighing Scrap at Receipt**

Weigh scrap at time of physical receipt in the DRMO using DRMS Form 146, an electronic weigh ticket or the DTID.

C4.6.2.3.2. **Inspection/Weighing Procedures**

C4.6.2.3.2.1 Inspect vehicles entering a DRMS field activity for the purpose of removing property by weight for extraneous cargo or suspicious items that could be used to inflate their weight. Re-inspect on departure, to ensure that all cargo and personnel in the vehicle at the time of weigh in are present on weigh out.

Section 1, Chapter 2, C2.15.5.1 and Section 2, Chapter 6, C6.9.3.5 require vehicles entering the scrap yard be inspected and weighed, in the AOR and elsewhere (in CONUS), unless an exception is provided in writing.

Recommendation 2: Ensure that site chiefs obtain the required annual inspections for all scales (or a waiver).

Response: Concur

A Statement of Work was submitted to obtain a contract for the annual inspection for scales at applicable sites in Afghanistan. A contract for providing the certified calibration of scales is expected to be in place no later than **January 13, 2013.**

Recommendation 3: Identify training for all pre-deployed personnel to receive in order to ensure employees understand most position requirements and to create a cross- leveled workforce.

Response: Concur

Training requirements are currently listed in the training plans of all employees deployed in the Civilian Expeditionary Workforce (CEW); and deployment training requirements for all CEW employees are listed in the DLA Learning Management System (LMS). Additionally, a "boot camp" of hands-on deployment training for CEW employees is in development. We anticipate the first training date to be **May 11-24, 2013.** This beneficial training will include all duties
CEW employees will encounter once they arrive on site, ready to begin work.

Recommendation 4: Develop a database to track certification and verification records of items with offensive or defensive military capabilities and requiring demilitarization actions.

Response: Concur

The OIG found one site could not identify a few items (from the sample selected for testing). Completing the Self-Assessment (SA) we require of supervisors will correct the problem. The OIG agreed that adding a database would be cumbersome and not likely improve the ability of the Afghanistan site or DLA Disposition Services to maintain required documents. Starting on **November 30, 2012.** the local Site Chief will verify the identified process in accordance with the quarterly SA in the Compliance Assessment Management System (CAMS) to ensure Demil documents are appropriately filed.

Demilitarization Coding

Recommendation 5: Establish procedures in the controlled Property Verification Office to periodically perform a review of items with integrity code 4, as well as "downgrade to scrap" transactions, to determine if DEMIL codes are accurate.

Response: Concur

We maintain accountability of all demil-required property. A new, enhanced process was added **April 30, 2012.** The Controlled Property Verification Office (CPVO) reviews weekly all National Stock Numbers (NSNs) received into the DLA Disposition Services inventory for DEMIL code accuracy. The CPVO reviews NSNs with integrity code 4; and, the DEMIL Verification at Receipt (DVR) process includes all DEMIL B and Q NSNs with integrity code 4. Downgrades to scrap transactions are reviewed for DEMIL code accuracy at the receipt stage as part of the review. At our field locations, if an unusual item is noticed in a scrap pile at a particular site, it is pulled out immediately as part of the management of the scrap pile process.

Contract Administration

Recommendation 6: Assign each site chief Contracting Officer's Representative responsibilities for the labor contract and provide monthly evaluations and update policies to the Contracting Officer.

Response: Concur

The COR oversight process was changed on (or about) **May 30, 2012** as a result of the finding leading to this recommendation. Each Site Chief now obtains the defined Defense Acquisition University (DAU) required training before entering Afghanistan. Once on site, the incoming Site Chief attends the required training (as assigned by the Contracting Officer) that can only be obtained in country. Now, each Site Chief is assigned Contracting Officer Representative (COR) for the labor contract in effect for their site. Each COR provides monthly evaluations to the Contracting Officer. The contracting office for the DLA Disposition Services labor contract in Afghanistan is the Army Regional Contracting Office in Bagram. This follow-on Army contract will soon be replaced by a new DLA Disposition Services contract (projected to be in place by July 2013) and will include these requirements:

1) A COR must be assigned at each site; and,
2) The CORs will be required to provide monthly status reports.

Recommendation 7: Conduct periodic refresher training with the contract personnel on site to ensure new and existing DOD and DLA policies are understood and followed over the course of operations.

Response: Concur

To address this concern, each site implemented a "receiver" (contract employee) training on (or about) **October 7, 2012**. This class is held regularly, as needed, to discuss issues found during the previous weeks, as well as to instruct the contract employees on any new procedures or policies DLA implements.

Recommendation 8: Establish and implement written procedures for scrap contractor- required support concerning installation access. Procedures should identify who is an authorized recipient of DLA-signed memorandums, and acceptable methods to provide the memorandums to the contractor.

Response: Concur

A new procedure was implemented on (or about) **October 7, 2012**. In order to standardize the process, all sites will now follow this same procedure: The access letter is provided to the company's authorized representative either in person; or, scanned and e-mailed to the company ahead of the date of required access needed. DLA letters of access apply directly to a driver's Teskara (unique personal identification) and are for a defined period of performance as referenced in the fetter. Each site has a file of each letter of access approved by the installation. The access procedures followed by DLA will be uniform in procedure. Access to the actual base, however, will be entirely dependent on the requirements and procedures followed at each location by base personnel. DLA will coordinate with each location's base personnel to insure compliance with base requirements while assuring effective but secure access for its contractors.

Equipment

Recommendation 9: Develop and implement performance metrics to track the length of time Material Handling Equipment is out of service to ensure the contractor performs according to contract requirements.

Response: Concur

Beginning in December of 2011, equipment readiness became an item of discussion in a weekly DLA Disposition Services maintenance teleconference. This meeting includes site chiefs, on-site maintainers, DSD-Central staff, a contracting representative, DLA Installation Support representatives, and the appropriate staff from DLA Disposition Services. (Sample slide packets are available, if requested by OIG).

The DSD-Central Equipment Readiness/Remediation Team (ERT) started tracking equipment down time on 15 January 2012). Tracking includes:

a) when the equipment is first reported non-operational;
b) what is at fault with the equipment;
c) the estimated repair completion date;
d) order status; and,
e) other pertinent information.

People are in place and process and performance metrics have been established to remedy this finding. On (or about) **June 15, 2012**, we started tracking contractor performance to ensure equipment down time is minimized, and the contractor, Relyant, is accountable for timely repairs. Specifically, our contract with Relyant currently gives them 120 hours to respond once we notify them of the need for unscheduled maintenance. Once we present the
property for repair, Relyant has 3 days to complete the repair. If the work is not completed in 3 days, Relyant must provide valid reasons to the COR/CO. If the delay is due to parts not available, Relyant has 120 hours once the part arrives to finish the repair.

<u>EDRT Mission, Utilization, Training, Communication</u>

Recommendation 10: Develop and implement standard operating procedures for the EDRT program, to include program expectations, metrics to measure success, and examples of standardized reports and training materials for the sites.

Response: Concur

Currently (as of November 15, 2012), EDRT teams across the Combined Joint Operations Area (CJOA) use Standard Operating Procedures (SOPs) and training programs that were aligned for the entire CJOA, not solely for Afghanistan deployment. To remedy this, the DSD- Central is staffing a separate draft CJOA-wide EDRT SOP. This new, revised SOP will place focus on Afghanistan-centric roles and responsibilities, command and control, missions, operational checklists, reporting requirements, and measures of performance and effectiveness. The DSD Central will take these steps toward completion:

15 November 2012: Vet final draft EDRT SOP across the DLA Disposition Services team:
15 December 2012: Complete the coordinated EDRT SOP; and,
15 January 2013: Release final EDRT SOP to workforce (and provide a copy to the OIG).

Recommendation 11: Update pre-deployment EDRT training to focus on current operations in Afghanistan, also incorporating EDRT standard operating procedure guidance.

Response: Concur

Afghanistan specific training was recently added to the EDRT pre-deployment training regimen as a result of this finding. DLA Disposition Services believes it is important that the EDRT training program continue to involve a well-rounded curriculum so EDRTs have the skillsets they need to operate in any environment (including and beyond Afghanistan). We are striving to train well-rounded, technically and tactically agile EDRTs, for both current and future operating environments. Also, as indicated in our response to Recommendation 10, the current EDRT training regimen is for the CJOA, not only Afghanistan. The new EDRT SOP will help to focus EDRT personnel, once they arrive on site, to work in Afghanistan. Pre- deployment training modifications are in the progress; and, (beginning in **January 15, 2013),** the EDRT annual training program will be modified to include Afghanistan-specific topics.

Recommendation 12: Establish appropriate communication methods between EDRTs and the sites, which minimizes operational security issues with the transmittal of potentially sensitive information.

Response: Concur

As a result of this finding, standardized procedures were put into place on **June 15, 2012** to ensure EDRTs operating in the AOR do not use open, non-encrypted email. EDRTs are now required to employ service "For Official Use Only" (FOUO) email platforms such as Defense Knowledge Online or Army Knowledge Online. EDRT training and the new, draft EDRT SOP both include communication security protocols and guidance concerning OPSEC concerns. EDRT personnel are equipped with satellite telephones to ensure they have continued voice communications even when there is no cell coverage.

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

March 24, 2014

MEMORANDUM FOR DIRECTOR, FINANCE
DIRECTOR, DLA INSTALLATION SUPPORT

SUBJECT: Rescission of DLA OIG audit report on Real Property Additions, Disposals, and Construction in Progress (DAF-12-15)

In December 2012, DLA OIG issued our final report on Real Property Additions, Disposals, and Construction-in-Progress. The original audit identified control deficiencies over the process of recording and accounting for additions and disposals of real property and assets under construction. We initially concluded that these deficiencies, taken as a whole, may represent a material weakness over the real property and construction in progress financial reporting process. Specifically, the deficiencies resulted in the lack of accountability over real property acquired and disposed of, unreliable financial information for managing day-to-day operations, and the possibility of misstatement of real property balances. DLA Finance and DLA Installation Support agreed with the findings and recommendations and began implementing the nine recommendations in the report.

In November 2013, DLA OIG initiated a quality assurance review to internally assess our compliance with generally accepted government auditing standards and internal policies and procedures at the project level – and this report was selected for detailed review. The ongoing quality assurance review has concluded that the initial audit work was deficient because the original audit team did not evaluate the effectiveness of information systems controls, and wrote recommendations that did not flow logically from the findings or were not directed at resolving the root causes identified in the report.

Therefore, effective immediately, I am rescinding audit report DAF-12-15, Audit of Real Property Additions, Disposals, and Construction in Progress. Recipients of the report should determine if the reportable conditions may assist management on identifying and driving improvement opportunities of real property assets under construction. Although seven of the nine recommendations have been implemented and are either closed or closed not verified, all nine recommendations will be removed from follow-up tracking.

Steven Pegott

STEVEN D. PIGOTT
Deputy Inspector General
DLA OIG Audit Division

DLA Office of the Inspector General

Audit of the DLA Managers' Internal Control Program

Audit Report: DLAOIG-FY15-05 **May 22, 2015**

MISSION

The DLA Office of the Inspector General Audit Division provides DLA leadership with sound advice and recommendations to assist them in making informed decisions to improve support to the warfighter, and proper stewardship of resources while remaining independent and objective in our auditing approach.

VISION

Motivated and trusted audit professionals who provide timely and value-added audit services emphasizing collaboration with management, risk mitigation and accountability.

Suggestion for Audits

To suggest or request audits, contact the office of the Deputy Inspector General for Auditing at OIG_Audit@dla.mil.

DLA ENTERPRISE HOTLINE

Report Suspected Fraud, Waste, Abuse or Mismanagement

https://www.dla.mil/DA
DLAEnterpriseHotlineProgram@dla.mil
DLA HQC, Suite 2358
1-800-411-9127

or contact the Department of Defense Hotline
1-800-424-9098 www.dodig.mil/hotline

DEFENSE LOGISTICS AGENCY
DEPARTMENT OF DEFENSE
hotline
make a difference

YOU MAY REMAIN ANONYMOUS

Acronyms Used

AUM	Assessable Unit Manager
DLAI	Defense Logistics Agency Instruction
ERM POC	Enterprise Risk Manager Point-of-Contact
FMFIA	Financial Managers Financial Integrity Act
GAO	Government Accountability Office
MICP	Managers’ Internal Control Program
MICA	Managers Internal Control Administrator
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PLFA	Primary Level Field Activities
SOA	Statement of Assurance

Report No. DLAOIG-FY15-05 (Project No. FY14-DLAOIG-14) May 22, 2015

Executive Summary: Audit of the DLA Managers' Internal Control Program

What We Did and Why

Our audit objective was initially to determine if DLA effectively identified and implemented internal controls over operations, financial and information system risks. However, because the Audit Readiness Initiative focused on controls over financial statement reporting and IT controls, we narrowed our scope of work and focused our audit efforts only on internal controls for operational processes. As result, our results only address internal control for operations and we did not opine on financial and information system controls. This audit was requested by J5.

What We Found

We determined that DLA has not effectively implemented the Managers' Internal Control Program (MICP) for operational risks in accordance with OMB Circular A-123. We judgmentally selected five audit reports issued by DODIG during FY 2012 –FY 2013 that identified internal control weakness in DLA's operational processes and found that three out of five process owners did not adhere to OMB Circular A-123 for reporting, tracking, and correcting those weaknesses. This condition occurred because:

- DLA senior leaders did not promote the MICP as an Agency priority.
- J5 did not fully execute the MICP. Specifically, J5 personnel did not make sure assessable unit managers and management internal control administrators understood their MICP responsibilities, which included identifying risks over operational processes; developing, implementing, and testing internal controls for operational processes; and maintaining documentation to support internal control test and annual statement of assurance submissions to J5.

What We Recommend

Our report contains five recommendations addressed to the Director, Strategic Plans and Policy (J5). These recommendations will improve the implementation and execution of the MICP.

Management Comments and Our Response

J5 fully concurred with four of five of our recommendations and partially concurred with one recommendation. We evaluated management's responses and found that the responses meet the intentions of our recommendations.

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

May 22, 2015

MEMORANDUM FOR DIRECTOR, DLA STRATEGIC PLANS AND POLICY (J5)

SUBJECT: Final Report – Audit of the DLA Managers' Internal Control Program

This is the final report on the Audit of the DLA Managers' Internal Control Program. The objective of the audit was initially to determine if DLA effectively identified and implemented internal controls over operations, financial and information system risks. However, our audit work focused on internal controls for operational process risks because DLA's audit readiness initiative concentrated on financial and information systems. As result, our results only address internal control for operations risks and we did not opine on internal controls for financial and information system risks.

We determined that DLA has not effectively implemented the Managers' Internal Control Program (MICP) for operational risks in accordance with OMB Circular A-123. We judgmentally selected five audit reports issued by DODIG during FY 2012 –FY 2013 that identified internal control weakness in DLA's operational processes and found that three out of five process owners did not adhere to OMB Circular for reporting, tracking, and correcting those weaknesses.

Based on our findings, we made five recommendations addressed to the Director, DLA Strategic Plans and Policy (J5) to improve the operations of the Managers' Internal Control Program. We requested and obtained management comments on a draft of this report. Verbatim management comments are included in Appendix C of this report. We will perform follow-up procedures after corrective actions are implemented and supporting documentation made available.

We appreciate the courtesies and cooperation extended to us during the audit. For additional information about this report please contact Ms. Tamonie Denegall at 703-767-6263 or email at Tamonie.denegall@dla.mil.

Steven Pigott

STEVEN D. PIGOTT
Deputy Inspector General
DLA OIG Audit Division

CONTENTS

Introduction

Appendices

INTRODUCTION

OBJECTIVE AND CONCLUSION

The objective of the audit was initially to determine if DLA effectively identified and implemented internal controls over operations, financial and information system risks. However, our audit work focused on internal controls for operational process risks because DLA's audit readiness initiative concentrated on financial and information systems. As result, our results only address internal control for operations risks and we did not opine on internal controls for financial and information system risks.

To determine whether DLA effectively identified and implemented internal controls over operations risks, we reviewed five DODIG audit reports that identified internal control weakness within DLA and annual statements of assurance for the periods FY 2012 and FY 2013. We determined that DLA has not effectively implemented the Managers' Internal Control Program (MICP) for operational risks. This condition occurred because:

- DLA senior leaders did not promote the MICP as an Agency priority. The senior leaders did not understand the tenets of MICP thereby causing a fractured process that only focused on controls over financial statements.

- J5 officials did not fully execute their duties. Specifically, J5 officials did not make sure assessable unit managers and management internal control administrators understood their responsibilities in the MICP process which included:

    - Identifying risks over operational processes.
    - Developing, implementing, and testing internal controls for operational processes.
    - Maintaining documentation to support internal control tests and annual statement of assurance submissions to J5.

As a result, the Statements of Assurance signed by the DLA Director may not be fully supported and may not accurately reflect operational risks. Our recommendations to address this finding begin on page 11 of this report.

BACKGROUND

This audit was conducted at the request of J5.

On April 30, 2009, the DLA Director signed General Order 9-09 transferring the MICP to DLA Strategic Planning and Enterprise Transformation (J5). The General Order states that the reporting requirements, program administration, and personnel support at the assessable unit level will be provided by DLA organizations, offices, and activities to accomplish enterprise Management Internal Control objectives. Additionally, administrative and personnel support will be provided by DLA organizations as appropriate.

Criteria

Federal Managers Financial Integrity Act of 1982 (FMFIA) This Act established the requirement for ongoing evaluations and reports on the adequacy of the systems of internal accounting and administration control. It mandated the Office of Management and Budget in consultation with the Comptroller General to establish guidelines for agencies to evaluate their systems of internal accounting and administration controls. These controls shall provide reasonable assurance that:

1. Obligations and costs are in compliance with applicable law.
2. Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation.
3. Revenues and expenditures are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

The Act also established a requirement for agency heads to report yearly on the compliance or non-compliance of those controls.

Office of Management and Budget (OMB) Circular A-123 (revised) OMB Circular A-123 dated December 21, 2004, titled “Management’s Responsibilities for Internal Control,” provides guidance to federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal controls. It is management’s responsibility to:

1. Develop and maintain effective internal controls.
2. Develop and execute strategies for implementing or reengineering agency programs and operations.
3. Design management structures that help ensure accountability for results.
4. Take systematic and proactive measures to develop and implement appropriate, cost-effective internal control.
5. Monitor and improve the effectiveness of internal controls associated with their programs. This continuous monitoring, and other periodic assessments, should provide the basis for the agency head’s annual assessment of and report on internal controls.

DoDI 5010.40 "Managers' Internal Control Program Procedures" This instruction dated May 30, 2013, assigned responsibility and prescribed execution procedures for the MICP. Specifically, the DoD and OSD component heads are responsible for establishing a MICP to:

1. Assess inherent risks in mission-essential processes.
2. Document and design internal controls.
3. Test the design and operating effectiveness of existing internal controls.
4. Identify and classify control deficiencies and promptly prepare and execute corrective action plans.
5. Monitor and report the status of corrective action plans until testing confirms resolution of identified deficiencies.

Defense Logistics Agency Instruction (DLAI) 5107 DLA's instruction requires DLA Strategic Plans and Policy (J5) to prepare the Annual Statement of Assurance (SOA) based upon input from Primary Level Field Activities (PLFA)/ J-codes. According to the DLAI 5107, the SOA will reflect the Agency's management internal control material weaknesses and plans of corrective actions, accounting system certification, and special interest items. Additionally, the DLAI 5107 requires that J5 establish reporting procedures to ensure that systems of management internal controls are implemented and operating as intended.

RESULTS AND RECOMMENDATIONS

The following section discusses the "Tone at the Top" set by DLA leadership for implementing and executing the MICP. We also discuss concerns with oversight of the MICP performed by J5 officials which included not making sure assessable unit managers (AUMs) and managers internal control administrators (MICAs) understood their roles and responsibilities in the MICP process which include identifying risks over operational processes; developing, implementing, and testing internal controls for operational processes; and maintaining documentation to support internal control test and annual statement of assurance submissions to J5.

Tone at the Top

DLA senior leaders did not promote the entire MICP as an Agency priority because they placed emphasis on the audit readiness initiative, which focused almost exclusively on financial and information technology controls.

According to OMB Circular A-123 and the Treadway Commission's Internal Control Integrated Framework, the first standard of internal control is the control environment. The control environment is where senior leaders establish "the tone at the top" regarding the importance of internal control including expected standards of conduct. Moreover, it is management's responsibility to reinforce expectations at the various levels of the organization.

During the audit, we searched for correspondence or publications issued by senior leadership that addressed MICPs importance to the Agency during FY 2012 and 2013. We were unable to locate any publications or memoranda that defined the "Tone at the Top" for DLA's MICP. Conversely, for the audit readiness initiative, senior leaders showed robust support by including the topic in the Director's Big Ideas and using various methods to communicate the importance of audit readiness to all Agency employees. Listed below are examples of the avenues that senior leaders used to promote audit readiness as the Agency's priority:

1. Established an Audit Readiness Help Mailbox.
2. Conducted over 13 "road shows"/town halls at PLFA's CONUS and OCONUS.
3. Published 10 DLA Today Articles.
4. Distributed posters, pamphlets and factsheets defining what audit readiness is.
5. Developed mandatory audit readiness training for all DLA employees that was available February 2013 (Audit Readiness 101).

Although not within the scope of this review, we located a memorandum signed in 2009 by a previous DLA Commander that stated he was committed to fostering a conscientious management climate supportive of internal control. Additionally the letter stated that a robust internal control program assures the Agency will avoid waste while maximizing the stewardship of resources. In contrast, the current Director signed a letter in February 2014 that focused on the importance of Audit Readiness and did not address MICP as a whole. The memorandum issued in February 2014 stated that DLA is taking steps to build the organization and structure that will ensure the Agency remains audit ready; and that every DLA employee needs to recognize the importance of Audit Readiness and be able to answer "What does Audit Readiness mean to me?"

Also, we asked five DLA senior leaders to give us their perspective in describing what the "Tone at the Top" was concerning MICP. Their views varied. One leader reported focusing on audit findings and implementing solutions and corrective actions as the "tone at the top" and two additional leaders agreed that there was good emphasis being placed on internal controls. However, one leader stated that MICP is viewed as a deliverable and another stated that at one time the MICP was viewed as a paper drill but the perception is changing as more focus has been placed on audit readiness.

Consequently, by not promoting MICP as an Agency priority, DLA senior leaders missed an opportunity to create a get well plan for its entire system of internal controls within the audit readiness initiative. Rather than exclusively focusing on internal controls over financial statements, senior leaders could have used this initiative to train employees on the tenets of MICP and developed an integrated approach to ensure operational processes had the necessary internal controls in place to mitigate risks as well as controls over financial statements.

DLA could address this issue by establishing the requirement in the DLAI 5107 that management internal control training on the tenets is mandatory for all DLA employees on an annual basis. DLA senior leaders should obtain training from subject matter experts from the Office of Management and Budget or the Government Accountability Office to better promote the tenets of the MICP and the importance of establishing internal controls. And the senior leaders could develop and communicate a comprehensive message that conveys the Agency's position and priority of the MICP and that the program is inclusive of all three (operations, financial and IT) requirements of the program within the enterprise yearly.

MICP Oversight and Responsibilities

J5 officials did not fully execute MICP oversight and responsibilities. Specifically, J5 officials did not make sure AUMs and MICAs understood their responsibilities in the MIC process which included:

1. Identifying risks over operational processes.
2. Developing, implementing, and testing internal controls for operational processes.
3. Maintaining documentation to support internal control tests and annual statement of assurance submissions to J5.

Operational Risks. Although, four of five assessable unit managers (AUMs) and process owners we interviewed identified high risk areas, we could not find a link between the self-identified high risk areas and the operational process or the internal controls weaknesses reported in DODIG audit reports.

MICP policies require management to:

1. Identify internal and external risks that may prevent the organization from meeting its objectives (or operational risks),
2. Consider relevant interactions within the organization as well as with outside organizations,
3. Analyze the potential effect or impact on the agency.

Internal and external risk can be identified by auditors, internal management reviews, or observations of noncompliance with laws and regulations.

Assessable unit managers at five separate DLA locations provided us documents that described high risk areas they identified for their respective locations for FYs 2012 and 2013. While we were able to track those risks to their associated annual operating plans and the narratives submitted as part of their individual internal control annual assurance statements -- for four of the five locations -- the high risks did not correlate to their operational processes and internal controls. For example, in FY2013, DODIG identified an internal control weakness over the process for conducting the joint reconciliation of offsetting fuel balances. The audit work was conducted in FY2012 when the PLFA listed its high risk areas as being: burden shifting, workforce retention and development, and warfighter support. In FY2013, the year the report was issued, the PLFA did not identify any risk areas. In both years, the only process the PLFA reported as tested were the internal controls over air card, which was not listed as a high risk area. In Appendix B, we show the weaknesses identified for the five DODIG reports we judgmentally selected for review, the high risks identified by the PLFAs and J-codes in their annual assurance statements, and the internal controls tested.

This analysis reflects that AUMs did not have a clear understanding of the direct correlation of identifying risks, considering the effects on the organization, and analyzing the effects. As a result, the AUMs may have tested and monitored internal controls that did not address high risk areas, thereby increasing the Agency's risk of mission failure.

DLA should address this issue by providing additional training to AUMs and process owners about MICP and the interrelated linkages between operational risk, operational processes, and internal controls. The training should also include a segment on coordinating with J5 officials on all internal control weakness identified by auditors and making the determination whether the internal control weakness is material and requires reporting in their annual statement of assurance submissions.

MICP Office. Although J5 officials provided training to the management internal control administrators and provided guidance to the PLFAs and J-codes for submitting individual internal control assessments – we found that J5 officials did not make sure:

1. AUMs maintained internal control plans and control test documentation to support annual assurance statements submitted to J5 for inclusion in the Agency's annual statement of assurance for FYs 2012 and 2013.
2. AUMs coordinated with J5 officials to determine the materiality of the internal controls weaknesses that DODIG identified in five audit reports we selected for review.

Moreover, J5 officials did not validate conclusions provided by the AUMs and MICAs on the effectiveness of the internal controls. This occurred because supervisory control for the AUMs and MICAs is at the PLFA and J-code level and the job of the J5 officials at the DLA headquarters level is to provide guidance and assistance when requested. Furthermore, the J5 MICP office did not have enough resources to travel to all of DLA's locations and validate the testing of numerous controls.

According to DODI 5010.40 and DLAI 5107, J5 officials are responsible for:

1. Maintaining internal control program documentation.
2. Reviewing reports received from all sources, including DoD IG audits and inspections and GAO reports and coordinating with field activities to determine if any discovered MIC deficiencies constitute material weaknesses.
3. Assisting in testing, as necessary and validating conclusions provided by subject matter experts on the effectiveness of the internal controls.

From our interview with an official from J5 and analyses of documentation provided by that official, we found that J5 office:

1. Did maintain statements of assurance submitted by the PLFAs and J-codes; however those statements contained unsupported conclusions. For example, in FY 2012, three PLFAs submitted statements of assurance with an unqualified level of assurance on their internal controls and in FY 2013, two PLFAs and one J-code did as well. However, the PLFAs and J-code did not maintain any documentation that showed operational internal controls had been tested. According to J5 officials, they did review submissions and asked questions about data that appeared to be inaccurate or unsupported – however, they did not validate that submissions were accurate. We reviewed a total of 10 statements of assurance submitted to J5 by three PLFAs and two J-codes for FYs 2012 and 2013 and found that activities could only provide us with the internal control plans but not the control test documentation to support their statements of assurance.
2. Did not coordinate with J-codes and PLFAs and review internal control weaknesses identified by audit organizations. We judgmentally selected five DODIG reports issued in FYs 2012 and 2013 that contained internal control weaknesses in the areas of logistics, contracting, and energy. J5 officials did not coordinate with the PLFAs and J-codes on the five internal control weaknesses identified by DODIG to determine whether the control weakness should have been reported as material weaknesses.

DLA could address this issue by having J5 officials confirm that AUMs and MICAs are conducting test of controls and maintaining support documentation for those tests. Additionally, have the J5 officials conduct random samples of submitted statements of assurance to validate and certify that the PLFA and J-codes annual assurance statement submissions are accurate and fully supported before including the submissions into the Agency's statement of assurance.

Assessable Unit Manager. We found that while DLA had appointed AUMs at all locations, they were not appointed to the correct level in the organization. Moreover, process owners –

who actually performed the role as an AUM – did not maintain documentation to support internal control testing. This occurred because the AUMs and process owners did not have a clear understanding of the program requirements.

Responsible personnel in J5 assigned the role of AUM to the Commanders and Directors of the PLFAs and J-codes. According to the DODI 5010.40, the AUM is responsible for:

1. Assessing risks affecting the assessable unit's mission or operations.
2. Identifying internal control objectives for that unit.
3. Reviewing processes and procedures to provide recommendations for enhancement, elimination, or implementation of assessable unit internal controls.
4. Testing the effectiveness of the internal controls.
5. Developing corrective action plans.
6. Maintaining MICP documentation in a central location to efficiently provide documents to the MICP coordinator as requested.

While Commanders and Directors do retain overall authority and responsibility for their MICP, the Commanders and Directors do not actually perform the duties of the AUM. For example, when we interviewed the PLFA Commanders and J-code Directors about their involvement with the MICP and the actions taken on the control weaknesses identified by DODIG audit reports- the Commanders and Directors directed us to speak with the process owners. The Commanders and Directors explained that they worked with the enterprise risk managers and process owners to identify high risk areas and the process owners kept them apprised of MICP issues. At the required time they reviewed the annual assurance statement submission and signed it.

Additionally, to determine whether the DLA's MICP was meeting the basic requirements of OMB Circular A-123 and DODI 5010.40, we asked process owners for documentation to support internal control testing they performed to support their FY 2012 and FY 2013 annual assurance statement submissions. The process owners told us that they performed test of controls but did not have any documentation to support the test they performed.

DLA could address these issues by:

1. Designating operational process owners as sub-AUMs.
2. Providing training to the AUMs on identifying risks and linking those risks to the associated operational processes.
3. Having the MICP coordinator meet with AUMs and review all control weaknesses identified via audits and investigations and determine whether those weaknesses should be deemed material and captured and reported; and
4. Confirming that AUMs and MICAs are conducting test of controls and maintaining support documentation for those tests.

Management Internal Control Administrators. We found that the DLAI did not specifically address the duties of the MICA; rather the policy only stated that each PLFA and J-code will designate one. This occurred because J5 did not include those duties when updating the DLAI in September 2009. As a result only one of the five MICA's performance standards we reviewed had a MICP objective.

According to J5 officials, the MICA is responsible for maintaining MICP documentation (e.g., process flows and narratives), and verifying and validating internal control testing results. However, the DLAI does not specifically address the duties of the MICA. The DLAI only states that the PLFA and J-codes will designate a MICA for all MICP matters. We interviewed the five MICAs assigned to the PLFAs and J-codes that had the internal control weaknesses identified by DODIG, and found that they did not:

1. Maintain supporting documentation for the PLFAs and J-codes annual statement of assurance statements submitted to J5.
2. Validate and verify tests of internal controls performed by AUMs/process owners.

Additionally, four of the five MICAs were unsure of their duties and responsibilities.
DLA could address this issue by updating the DLAI 5107 to make sure the instruction is aligned with the DoDI 5010.40 to outline the duties of the MICA.

Recommendations for Director, DLA Strategic Plans and Policy (J5)

Recommendation 1. Update DLAI 5107 to require annual training for DLA personnel on the DLA's Management Internal Control Program. Specifically, DLA Strategic Plans and Policy should provide training to the:

a. DLA Director and DLA senior leaders on the tenets of the Manager's Internal Control Program as prescribed by OMB Circular A-123 and DODI 5010.40. Use subject matter experts from the Office of Management and Budget or Government Accountability Office to provide the training.

b. Assessable unit managers and process owners on: (1) identifying risks and linking those risks to the associated operational processes, (2) coordinating with J5 on all control weaknesses identified via audits and investigations and determining whether those weaknesses need to be identified as material and captured, reported and tracked, (3) conducting test of controls and maintain support documentation for those tests.

c. Management internal control administrators on their responsibilities of validating and verifying tests of internal controls performed by assessable unit managers; and maintain supporting documentation for the PLFAs and J-codes annual statement of assurance.

d. DLA employees on the importance of MICP and how their everyday responsibilities contribute to the success of the program.

Management Comments: Concur. J5 has prepared the MICP Concept of Operations (CONOPs) and is coordinating for the Vice Director's signature. J5 is revising the DLAI 5107 to mirror the Department of Defense Instruction (DODI) 5010.40 "Managers' Internal Control Program Procedures" to include training requirements for DLA Director, DLA senior leaders, Assessable Unit Managers, process owners, Managers' Internal Control

Administrators (MICAs) and DLA employees. The OSD MICP Coordinator provided training for DLA senior leaders in December 2014, and refresher training is required annually. In November 2014, January and March 2015, J5 provided MICAs with phase I, II, and III training on their responsibilities for validating and verifying tests of internal controls and supporting documentation.

DLA OIG Response: Management's comments are responsive and meet the intent of our recommendation.

Recommendation 2. Coordinate with DLA, Director and DLA's senior leaders to develop a comprehensive message that conveys the Agency's position on the Manager's Internal Control Program. This message should clarify that the program is focused on operational, financial, and information system controls and detail the annual requirements to test and assert to internal controls over key processes and risk areas.

Management Comments: Concur. The DLA Director signed the FY15 DLA MICP "Tone at the Top" memorandum on October 21, 2014. The memorandum was disseminated to the Executive Board on October 23, 2014. The way-ahead strategy established by J5 is to have the "Tone at the Top" memorandum signed by the DLA Director and published in the 4th quarter of each fiscal year. The memorandum will detail the focus and the scope of the MIC program for the upcoming fiscal year. The FY2016 "Tone at the Top" memorandum is in coordination for the DLA Director's signature. The memorandum clarifies that the MIC program is focused on operational, financial and information systems internal control evaluation. Additionally, DLA J5 will periodically post information on the Commander's Blog about the MICP to ensure continued visibility and focus.

DLA OIG Response: Management's comments are responsive and meet the intent of our recommendation.

Recommendation 3. Develop and implement a plan to conduct random samples of statements of assurance submitted by PLFAs and J-codes to validate and certify that the annual assurance statement submissions are accurate and fully supported before including the submissions into the Agency's statement of assurance. This should include verifying that the assessable unit managers conducted tests of internal controls and the management internal control administrators validated those tests and maintained supporting documentation.

Management Comments: Concur. In FY2015, J5 began providing feedback to MICA's to validate that their respective statements of assurance are fully supported before submitting to J5 for inclusion into DLA's statement of assurance. J5 requested a status update from the MICA's in February 2015 to determine what progress had been made on testing processes that had been identified as high risk areas. As a result of the status update, J5 provided feedback to the MICA's for their statement of assurance submissions prior to the May 29, 2015 deadline for assertion letters from their respective PLFAs and J/D-codes. J5 will continue to verify and validate the accuracy of the statements of assurance submissions. The requirement to validate the accuracy of the statements of assurance before submitting to J5 will be reflected in the DLA 5010.40 policy (DLA 5010.40 will replace the DLAI 5107).

DLA OIG Response: Management's comments are responsive and meet the intent of our recommendation.

Recommendation 4. Designate operational process owners as sub-assessable unit manages.

Management Comments: Partial-Concur. An assessable unit (AU) is any organizational, functional, and programmatic or other applicable subdivision that allows for adequate internal control analysis. An assessable unit manager (AUM) is a manager assigned direct responsibility for ensuring that an internal control system is in place and operating effectively within his/her assessable unit. At the Enterprise level, J5 defines AUMs as the Commander, Director and Enterprise Business Cycle Owners. At this level, the AUMs are responsible for assessing and asserting to the effectiveness of controls (Financial, Systems and Operational) over their processes. The AUMs have the authority to designate as many sub-assessable units/sub-assessable unit managers as deemed appropriate. Additionally, DLA J5 is working with the management internal control and enterprise risk management integration cell to standardize the definitions and terminology used throughout the agency specifically regarding AU, AUM, and MICAs.

DLA OIG Response: Although J5 partially concurred with the recommendation, their plan to standardize the definitions and terminology regarding AUs, AUMs, and MICAs along with the planned training for DLA senior leaders identified in J5's response to recommendation 1 will aid in clarifying the roles and responsibilities of the AUMs. This should result in the AUMs understanding the need to assign sub-assessable unit managers as needed to ensure internal controls within their processes are in place and operating effectively. Therefore, J5's response meets the intention of this recommendation.

Recommendation 5. Update DLAI 5107 to make sure it is in line with the current requirements prescribed by OMB Circular A-123 and DOD Instructions 5010.40 "Managers' Internal Control Program Procedures." Specifically, DLAI 5107 should:

a. Clearly describe the requirements of the MIC program to include identifying risks and controls over operations, financial statement reporting and information systems.
b. Clearly define the roles and responsibilities of DLA senior leadership, key personnel at the PLFAs and J-codes, J5 MIC program office, the assessable unit managers and the management internal control administrators.

Management Comments: Concur. J5 is currently revising the DLAI 5107 (the revised DLAI 5107 will become DLA Policy 5010.40) to mirror Department of Defense Instruction (DODI) 5010.40, "Managers' internal Control Program Procedures". The revised policy will clearly define the requirements of the MIC program to include identifying risks and controls over operations, financial statement reporting and information systems. The policy will also reflect the roles and responsibilities of DLA senior leadership, key personnel at the PLFAs and J/D-codes, J5 MIC program management office, the AUMs, EBCOs, and MICAs. Coordination of the revised policy is projected to start in August of 2015 and finalized within about six months.

DLA OIG Response: Management's comments are responsive and meet the intent of our recommendation.

APPENDIX A. SCOPE AND METHODOLOGY

On May 22, 2014, the DLA OIG announced the Audit of DLA's Manager's Internal Control Program (MICP). We conducted fieldwork for this performance audit from June 23, 2014 to September 30, 2014 in accordance with generally accepted government auditing standards (GAGAS) issued by GAO. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

To determine if DLA effectively identified and implemented internal controls over operations, financial and informational systems risks, we:

1. Obtained and reviewed the following guidance:
    a. Financial Managers Financial Integrity Act (FMFIA) of 1982.
    b. Office of Management and Budget (OMB) Circular A-123.
    c. Department of Defense Instruction (DoDI) 5010.40.
    d. Defense Logistics Agency Instruction (DLAI) 5107.
2. Interviewed personnel in DLA Acquisition, DLA Installation Support, DLA Finance, DLA Energy, DLA Aviation, DLA Land and Maritime, DLA Logistics Operations, and DLA Strategic Plans and Policy.
3. Selected the following five external audit reports that identified material internal control weaknesses:
    a. DODIG-2013-117 "*Enhanced Oversight Needed for Nontactical Vehicle Fleets in the National Capital Region*"
    b. DODIG-2012-049 " *Improvements Needed with Identifying Operating Costs Assessed to the Fleet Readiness Center Southwest*"
    c. DODIG-2013-073 "*Use of Defense Logistics Agency Excess Parts for High Mobility Multipurpose Wheeled Vehicle Deport Repairs will Reduce Costs*"
    d. DODIG-2013-101 "*Fuel Exchange Agreement Reconciliations are Effective, but the Joint Reconciliation Process Needs Improvement*"
    e. DODIG-2013-090 "*Improved Guidance Needed to Obtain Fair and Reasonable Prices for Sole-Source Spare Parts Procured By the Defense Logistics Agency From the Boeing Company*"
4. Reviewed the annual Statement of Assurance for DLA, PLFA and J-codes statements of assurance, and the Annual Operating Plan (AOP) created locally by each PLFA/J Code for FY12 to first quarter FY14.
5. Interviewed the Manager's Internal Control Administrator (MICA), Enterprise Risk Manager Point of Contact (ERM POC), and the Assessable Unit Manager (AUM) for five (5) PLFA/J Codes whose report was selected for testing.
6. Reviewed internal control supporting documentation to determine reasonableness of the control testing.

Scope

We used prior audit reports from external audit agencies to answer our objective because the audit reports identified specific internal control weaknesses for PLFAs and J-codes.
To determine the completed audits performed by the DoD IG and GAO that noted internal control weaknesses at DLA, we contacted the DLAOIG External Audit Liaison. The External

Audit Liaison identified 20 external audit reports that had internal control weaknesses for DLA. We judgmentally selected five out of the 20 reports to track the findings and issues and determine whether the failed controls surrounding the finding were included in the Statement of Assurance (SOA). We selected five reports because those reports represented a cross section of the DLA enterprise and its operational processes. We did not project the results obtained from the five reports across the entire population of 20 reports.

Use of Computer-Processed Data

We did not rely on computer-processed data for our findings, conclusions, or recommendations for this report. Many of the outputs used were manually created, and were not system produced.

Locations/Commands visited

- DLA Acquisition.
- DLA Installation Support.
- DLA Finance.
- DLA Energy.
- DLA Aviation.
- DLA Land and Maritime.
- DLA Logistics Operations.
- DLA Strategic Plans and Policy.

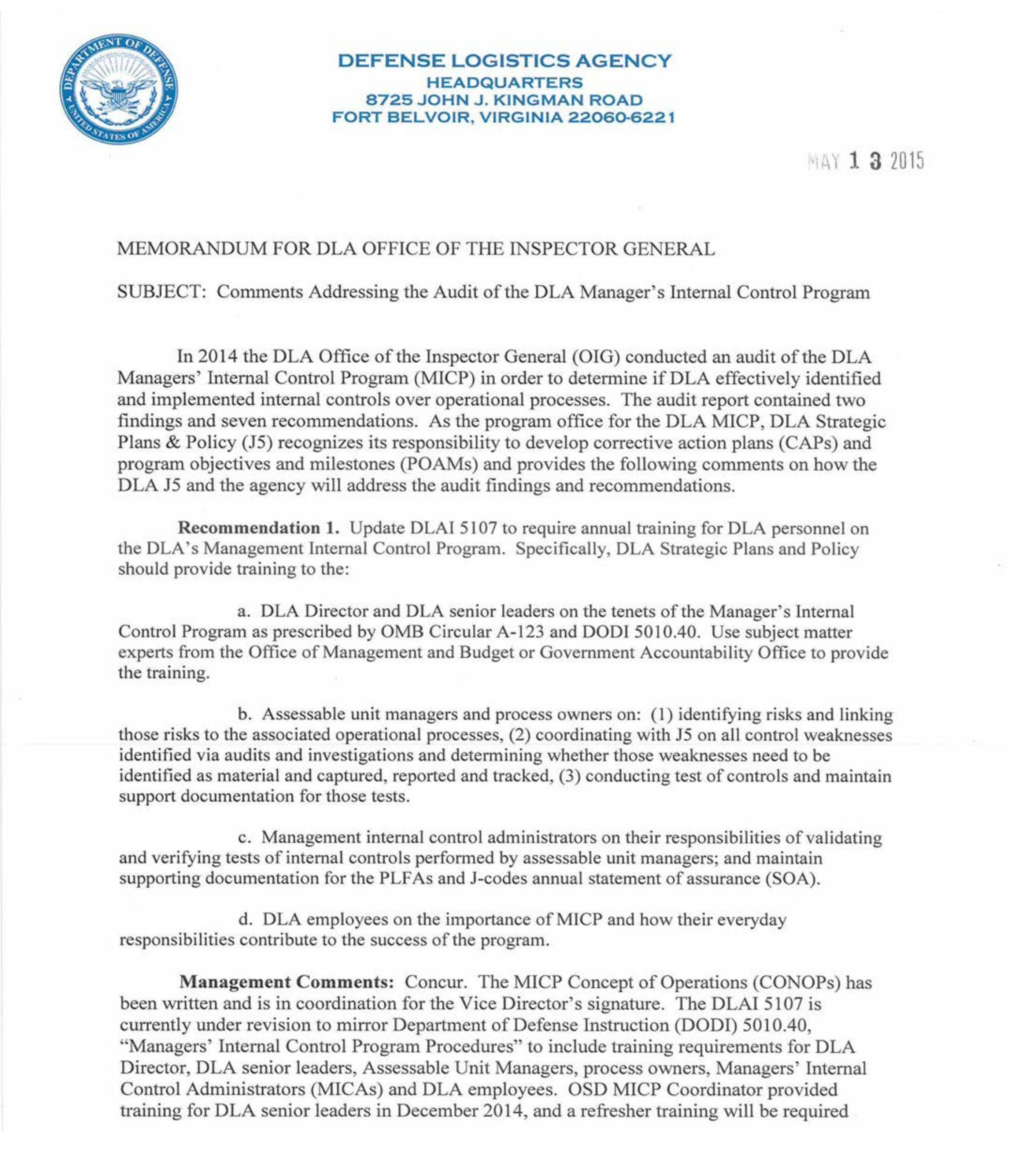
APPENDIX B. SUPPLEMENTAL INFORMATION

Comparison of Control Weakness to Data Reported in the Annual Assurance Statement

Audit Report Number	Internal Control Weakness Identified by DODIG Audit Reports	Risks Reported By PLFA and J-codes	Internal Controls Reported Tested in the Statement of Assurance
DODIG-2012-049	The Commander, DLA Aviation San Diego and the Director, DLA Finance Aviation did not have a local support agreement that clearly outlined the details of their partnership with the Fleet Readiness Center Southwest or written policies and standard operating procedures for developing or documenting estimated operating costs for FRCSW	**FY12** No risk assessment performed. **FY13** 1. Contracting Officers will not sign the 2579 - Small Business Coordination. 2. Contract file will not contain all required pricing documents. 3. Pricing Document will not contain a comparison of historical data to current offer/proposal.	**FY12** 1. High Dollar Obligations. 2. Contract File Contents. **FY13** 1. Depot Level Reparable Process Cycle Memorandum Validation and TOD. 2. Excluded Parties List System Printout in Files.
DODIG-2013-117	DLA had internal control weaknesses because they did not assess their requirements for nontactical fleet vehicles in the NCR.	**FY12** 1. Non-compliance with laws, regulations and policies. 2. Contractor performance could result in mission failure for the agency. 3. US industrial base cannot (or will not) support National Defense requirements, then DLA may fail to satisfy customer requirements. **FY13** 1. GPC Purchases. 2. Procurement Management Review Process.	**FY12** No control testing submitted. **FY13** 1. Reviewed one control in the GPC. 2. Reviewed PMR Process.

Audit Report Number	Internal Control Weakness Identified by DODIG Audit Reports	Risks Reported By PLFA and J-codes	Internal Controls Reported Tested in the Statement of Assurance
DODIG-2013-090	DLA Aviation contracting officers did not conduct a fair and reasonable price analysis for purchasing spare part items via sole source from Boeing.	**FY12** No risk assessment performed. **FY13** 1. Contracting Officers will not sign the 2579 - Small Business Coordination. 2. File will not contain all required pricing documents. 3. Pricing Document will not contain a comparison of historical pricing to the current offer/proposal.	**FY12** 1. High Dollar Obligations. 2. Contract File Contents. **FY13** 1. Depot Level Reparable Process Cycle Memorandum Validation and TOD. 2. Excluded Parties List System Printout in Files.
DODIG-2013-073	DLA did not assess DLA-owned HMMWV repair parts inventory at key contract decision points to maximize use of its own stock before purchasing parts through an ILP contract.	**FY12** 1. Parts availability and quality. 2. Standardization of shipyard. 3. Installation security, and threat reaction. **FY13** 1. Industrial Base Degradation. 2. Delivery of non-conforming or counterfeit parts. 3. Workforce Resiliency during period of reduced sales. 4. Wholesale/retail balance. 5. Force Protection compromise.	**FY12** No control testing submitted. **FY13** Submitted inspection report prepared by internal review as control test performed. However report was not clear as to processes inspected.
DODIG-2013-101	DLA Finance Energy's process for conducting the joint reconciliation by offsetting fuel balances did not obtain standard price value for the Italian Air Force Fuel Service Agreement balances for 2006 through 2010.	**FY12** 1. Burden Shifting (Warfighter Support). 2. Workforce Retention and Development. 3. Warfighter Support in Austere Areas. **FY13** No risk assessment performed.	**FY12** AIR Card Program **FY13** AIR Card Program

APPENDIX C. MANAGEMENT COMMENTS



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

MAY 13 2015

MEMORANDUM FOR DLA OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Comments Addressing the Audit of the DLA Manager's Internal Control Program

In 2014 the DLA Office of the Inspector General (OIG) conducted an audit of the DLA Managers' Internal Control Program (MICP) in order to determine if DLA effectively identified and implemented internal controls over operational processes. The audit report contained two findings and seven recommendations. As the program office for the DLA MICP, DLA Strategic Plans & Policy (J5) recognizes its responsibility to develop corrective action plans (CAPs) and program objectives and milestones (POAMs) and provides the following comments on how the DLA J5 and the agency will address the audit findings and recommendations.

Recommendation 1. Update DLAI 5107 to require annual training for DLA personnel on the DLA's Management Internal Control Program. Specifically, DLA Strategic Plans and Policy should provide training to the:

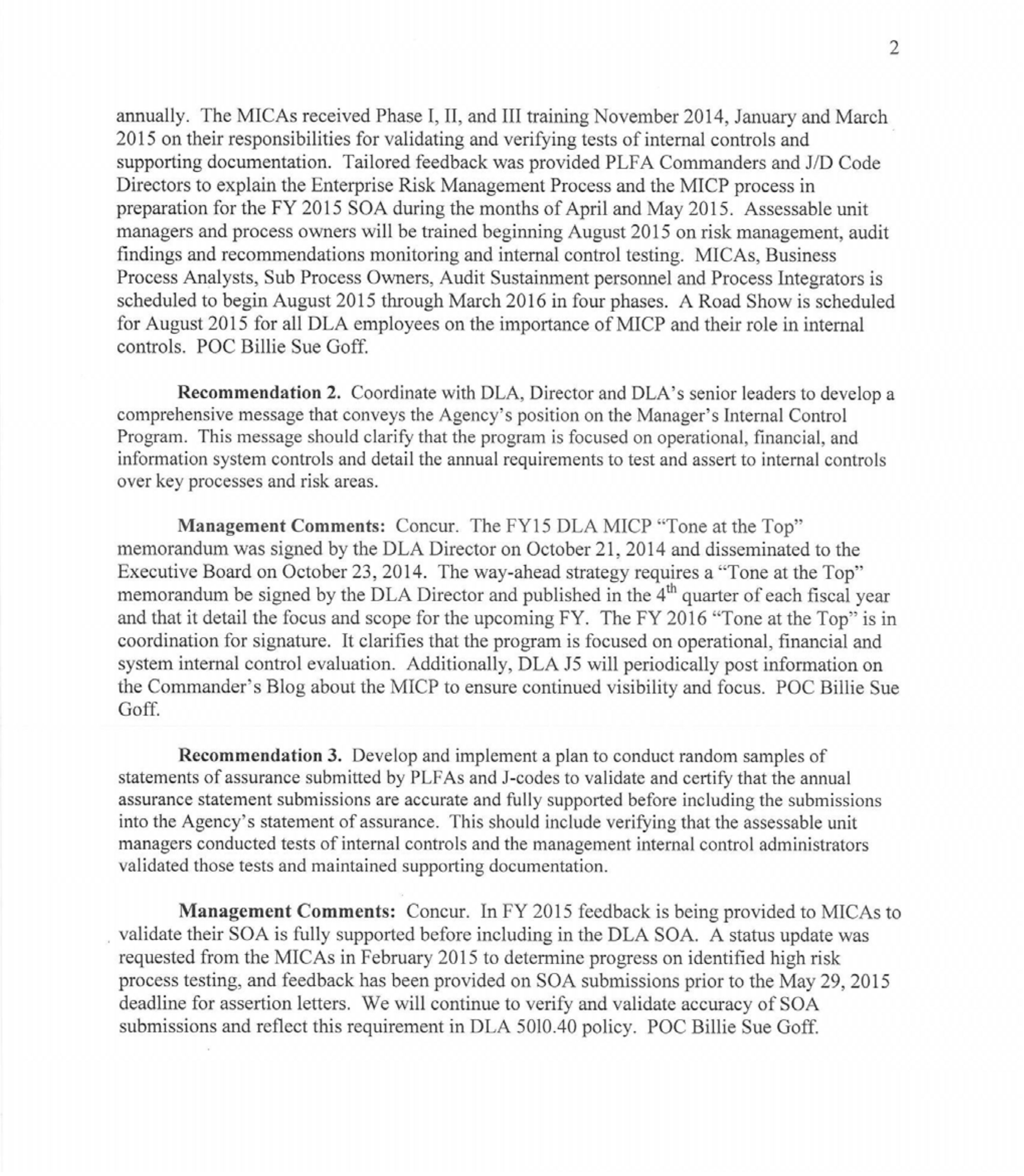
a. DLA Director and DLA senior leaders on the tenets of the Manager's Internal Control Program as prescribed by OMB Circular A-123 and DODI 5010.40. Use subject matter experts from the Office of Management and Budget or Government Accountability Office to provide the training.

b. Assessable unit managers and process owners on: (1) identifying risks and linking those risks to the associated operational processes, (2) coordinating with J5 on all control weaknesses identified via audits and investigations and determining whether those weaknesses need to be identified as material and captured, reported and tracked, (3) conducting test of controls and maintain support documentation for those tests.

c. Management internal control administrators on their responsibilities of validating and verifying tests of internal controls performed by assessable unit managers; and maintain supporting documentation for the PLFAs and J-codes annual statement of assurance (SOA).

d. DLA employees on the importance of MICP and how their everyday responsibilities contribute to the success of the program.

Management Comments: Concur. The MICP Concept of Operations (CONOPs) has been written and is in coordination for the Vice Director's signature. The DLAI 5107 is currently under revision to mirror Department of Defense Instruction (DODI) 5010.40, "Managers' Internal Control Program Procedures" to include training requirements for DLA Director, DLA senior leaders, Assessable Unit Managers, process owners, Managers' Internal Control Administrators (MICAs) and DLA employees. OSD MICP Coordinator provided training for DLA senior leaders in December 2014, and a refresher training will be required



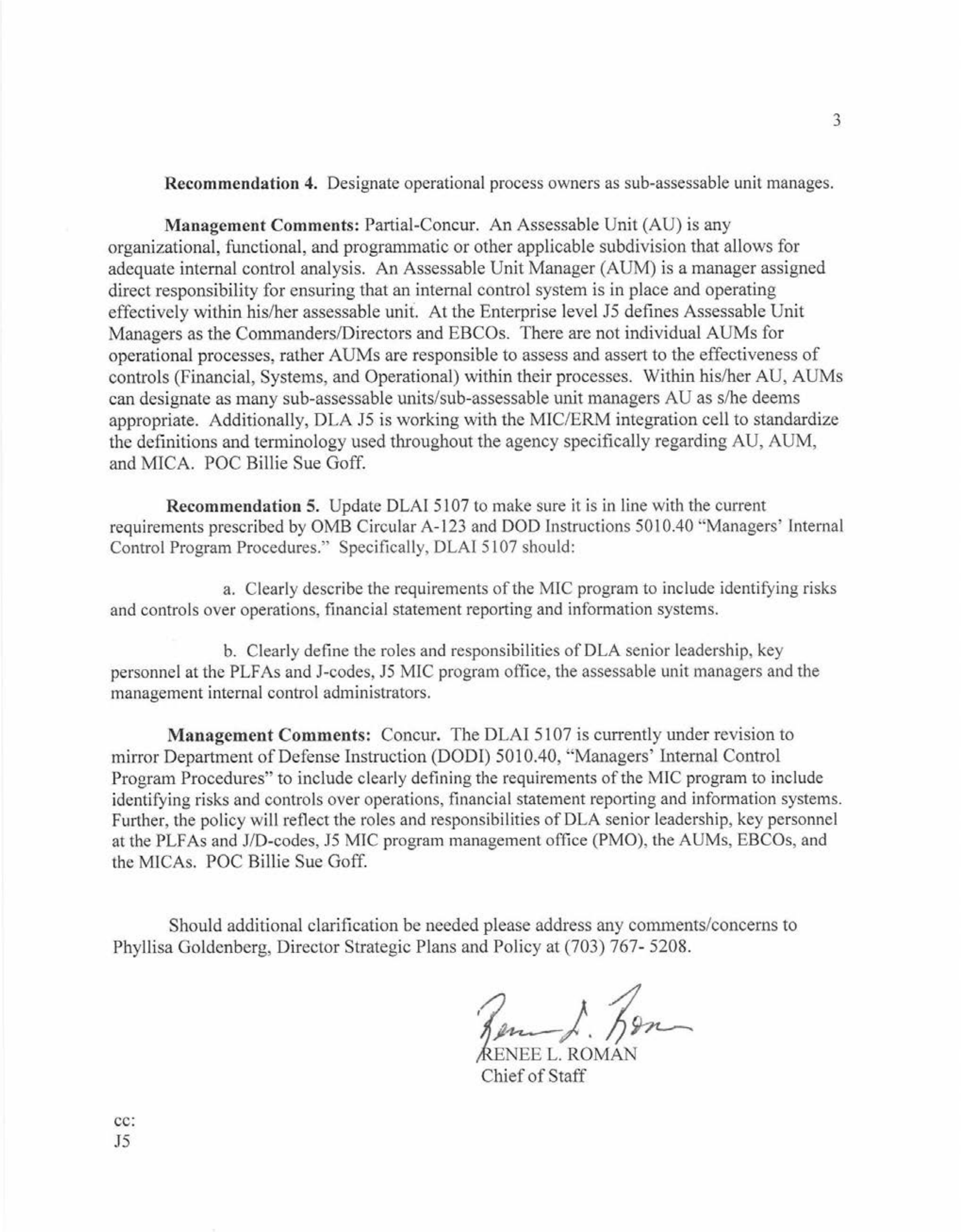
annually. The MICAs received Phase I, II, and III training November 2014, January and March 2015 on their responsibilities for validating and verifying tests of internal controls and supporting documentation. Tailored feedback was provided PLFA Commanders and J/D Code Directors to explain the Enterprise Risk Management Process and the MICP process in preparation for the FY 2015 SOA during the months of April and May 2015. Assessable unit managers and process owners will be trained beginning August 2015 on risk management, audit findings and recommendations monitoring and internal control testing. MICAs, Business Process Analysts, Sub Process Owners, Audit Sustainment personnel and Process Integrators is scheduled to begin August 2015 through March 2016 in four phases. A Road Show is scheduled for August 2015 for all DLA employees on the importance of MICP and their role in internal controls. POC Billie Sue Goff.

Recommendation 2. Coordinate with DLA, Director and DLA's senior leaders to develop a comprehensive message that conveys the Agency's position on the Manager's Internal Control Program. This message should clarify that the program is focused on operational, financial, and information system controls and detail the annual requirements to test and assert to internal controls over key processes and risk areas.

Management Comments: Concur. The FY15 DLA MICP "Tone at the Top" memorandum was signed by the DLA Director on October 21, 2014 and disseminated to the Executive Board on October 23, 2014. The way-ahead strategy requires a "Tone at the Top" memorandum be signed by the DLA Director and published in the 4th quarter of each fiscal year and that it detail the focus and scope for the upcoming FY. The FY 2016 "Tone at the Top" is in coordination for signature. It clarifies that the program is focused on operational, financial and system internal control evaluation. Additionally, DLA J5 will periodically post information on the Commander's Blog about the MICP to ensure continued visibility and focus. POC Billie Sue Goff.

Recommendation 3. Develop and implement a plan to conduct random samples of statements of assurance submitted by PLFAs and J-codes to validate and certify that the annual assurance statement submissions are accurate and fully supported before including the submissions into the Agency's statement of assurance. This should include verifying that the assessable unit managers conducted tests of internal controls and the management internal control administrators validated those tests and maintained supporting documentation.

Management Comments: Concur. In FY 2015 feedback is being provided to MICAs to validate their SOA is fully supported before including in the DLA SOA. A status update was requested from the MICAs in February 2015 to determine progress on identified high risk process testing, and feedback has been provided on SOA submissions prior to the May 29, 2015 deadline for assertion letters. We will continue to verify and validate accuracy of SOA submissions and reflect this requirement in DLA 5010.40 policy. POC Billie Sue Goff.



Recommendation 4. Designate operational process owners as sub-assessable unit manages.

Management Comments: Partial-Concur. An Assessable Unit (AU) is any organizational, functional, and programmatic or other applicable subdivision that allows for adequate internal control analysis. An Assessable Unit Manager (AUM) is a manager assigned direct responsibility for ensuring that an internal control system is in place and operating effectively within his/her assessable unit. At the Enterprise level J5 defines Assessable Unit Managers as the Commanders/Directors and EBCOs. There are not individual AUMs for operational processes, rather AUMs are responsible to assess and assert to the effectiveness of controls (Financial, Systems, and Operational) within their processes. Within his/her AU, AUMs can designate as many sub-assessable units/sub-assessable unit managers AU as s/he deems appropriate. Additionally, DLA J5 is working with the MIC/ERM integration cell to standardize the definitions and terminology used throughout the agency specifically regarding AU, AUM, and MICA. POC Billie Sue Goff.

Recommendation 5. Update DLAI 5107 to make sure it is in line with the current requirements prescribed by OMB Circular A-123 and DOD Instructions 5010.40 "Managers' Internal Control Program Procedures." Specifically, DLAI 5107 should:

a. Clearly describe the requirements of the MIC program to include identifying risks and controls over operations, financial statement reporting and information systems.

b. Clearly define the roles and responsibilities of DLA senior leadership, key personnel at the PLFAs and J-codes, J5 MIC program office, the assessable unit managers and the management internal control administrators.

Management Comments: Concur. The DLAI 5107 is currently under revision to mirror Department of Defense Instruction (DODI) 5010.40, "Managers' Internal Control Program Procedures" to include clearly defining the requirements of the MIC program to include identifying risks and controls over operations, financial statement reporting and information systems. Further, the policy will reflect the roles and responsibilities of DLA senior leadership, key personnel at the PLFAs and J/D-codes, J5 MIC program management office (PMO), the AUMs, EBCOs, and the MICAs. POC Billie Sue Goff.

Should additional clarification be needed please address any comments/concerns to Phyllisa Goldenberg, Director Strategic Plans and Policy at (703) 767- 5208.

RENEE L. ROMAN
Chief of Staff

cc:
J5

DLA Office of the Inspector General

Accountability of Government Furnished Equipment

Audit Report: DLA OIG-FY15-06 **June 11, 2015**

MISSION

The DLA Office of the Inspector General Audit Division provides DLA leadership with sound advice and recommendations to assist them in making informed decisions to improve support to the warfighter, and proper stewardship of resources while remaining independent and objective in our auditing approach.

VISION

Motivated and trusted audit professionals who provide timely and value-added audit services emphasizing collaboration with management, risk mitigation and accountability.

Suggestion for Audits

To suggest or request audits, contact the office of the Deputy Inspector General for Auditing at OIG_Audit@dla.mil.

DLA ENTERPRISE HOTLINE

Report Suspected Fraud, Waste, Abuse or Mismanagement

https://www.dla.mil/DA

DLAEnterpriseHotlineProgram@dla.mil

DLA HQC, Suite 2358

1-800-411-9127

or contact the Department of Defense Hotline

1-800-424-9098 www.dodig.mil/hotline

hotline@dodig.mil

YOU MAY REMAIN ANONYMOUS

Acronyms Used

APO	Accountable Property Officer
DCSO	DLA Contracting Services Office
DFARS	Defense Federal Acquisition Regulation Supplement
EBS	Enterprise Business System
FAR	Federal Acquisition Regulation
GFE	Government Furnished Equipment
GFP	Government Furnished Property
PGI	Procedures Guidance Instruction

Report No. DLAOIG-FY15-06 (Project No. FY14-DLAOIG-03) June 11, 2015

Executive Summary: Accountability of Government Furnished Equipment

What We Did and Why

The objective of our audit was to determine whether DLA properly accounted for government furnished equipment (GFE) provided to contractors.

What We Found

To determine whether DLA properly accounted for GFE provided to contractors, we focused this audit on preparing and maintaining GFE listings, recording the property in the Enterprise Business System (EBS) and linking the GFE to a specific contract. Because DLA could not provide a population of contracts containing GFE, we conducted our audit based on 17 contracts self-identified as containing GFE from three selected Acquisition Offices. We reviewed those 17 contracts and determined DLA did not properly account for GFE provided to contractors. Specifically, we noted:

- Acquisition personnel did not properly identify GFE and maintain GFE listings within a contract.
- GFE was not easily traceable from the contract to EBS for accountability purposes.

This occurred because contracting actions did not comply with Federal Acquisition Regulations and Defense Federal Acquisition Regulation Supplement requirements and DLA procedures to identify and account for GFE were not clearly defined. As a result, contracts did not properly identify the property offered to the contractor or changes to the actual property received. Additionally, DLA was unable to identify a definitive population of contracts providing GFE and ensure proper accountability of equipment in EBS. The results of this audit should be of concern to DLA because EBS information supports DLA's financial statements.

What We Recommend

Our report contains three recommendations addressed to the Director, DLA Acquisition and one recommendation to the Director, DLA Installation Support to improve the accountability of GFE. The details of the four recommendations are on page nine of this report.

Management Comments and Our Response

DLA Acquisition and DLA Installation Support concurred with the four recommendations. We evaluated management's responses and found that the responses meet the intentions of our recommendations.

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

June 11, 2015

MEMORANDUM FOR DIRECTOR, DLA ACQUISITION
DIRECTOR, DLA INSTALLATION SUPPORT

SUBJECT: Final Audit Report – Accountability of Government Furnished Equipment

This is the final report on the Audit of Accountability of Government Furnished Equipment. Our objective was to determine whether DLA properly accounted for government furnished equipment provided to contractors.

We determined DLA did not properly account for GFE provided to contractors. Specifically, we noted Acquisition personnel did not properly identify GFE and maintain GFE listings within a contract and GFE was not easily traceable from the contract to EBS for accountability purposes.

Based on our findings, we made three recommendations addressed to the Director, DLA Acquisition and one recommendation to the Director, DLA Installation Support. Verbatim management comments are included in Appendix B of this report. We will perform follow-up procedures after corrective actions are implemented and supporting documentation made available.

We appreciate the courtesies and cooperation extended to us during the audit. For additional information about this report please contact Ms. Kelly L. Donahue at 269-961-5422 or email at kelly.donahue@dla.mil.

Steven Pigott

STEVEN D. PIGOTT
Deputy Inspector General
DLA OIG Audit Division

CONTENTS

Introduction

Results and Recommendations

Appendices

INTRODUCTION

OBJECTIVE AND CONCLUSION

The objective of our audit was to determine whether DLA properly accounted for government furnished equipment (GFE) provided to contractors.

Because DLA could not provide a population of contracts containing GFE, we conducted our audit based on 17 contracts self-identified as containing GFE from three selected Acquisition Offices. We reviewed those 17 contracts and determined DLA did not properly account for GFE provided to contractors. Specifically, Acquisition personnel did not properly identify GFE and maintain GFE listings within a contract. In addition, GFE was not easily traceable from the contract to Enterprise Business System (EBS) for accountability purposes. This occurred because contracting actions did not comply with Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) requirements and DLA procedures to identify and account for GFE were not clearly defined. As a result, contracts did not properly identify the property offered to the contractor or changes to the actual property received and DLA was unable to identify a definitive population of contracts providing GFE and ensure proper accountability of equipment in EBS. This should be of concern to DLA because EBS information supports DLA’s financial statements.

Based on the results of our audit and the concerns related to internal controls, we will provide a copy of the final report to DLA Strategic Plans and Policy as part of the management internal controls for DLA.

BACKGROUND

Internal Controls. We determined the FY 14 DLA Statement of Assurance identified a material weakness related to the automated contract closeout process and return of Government Furnished Property to the government. In addition, the Statement of Assurance identified weaknesses in the Acquire to Retire assessable unit for controls and reconciliation failures for capitalized general equipment (greater than $250,000) due to lack of guidance and Agency-wide policies and procedures. DLA Installation Support explained that audit readiness efforts were focused on capitalized equipment and not Government Furnished Equipment. The two weaknesses identified in the FY 14 Statement of Assurance were not evaluated within the context of answering our audit objective. In order to answer our audit objective, we focused on GFE provided to contractors.

Government Furnished Property. Government furnished property (GFP) is property the government provides to a contractor for performance of a contract. There are different categories of GFP, such as material, equipment, special test equipment, or special tooling. Our audit focused on equipment provided to contractors. Equipment is a tangible item that is functionally complete for its intended purpose, durable, nonexpendable, and needed for the performance of a contract. GFE is specified in a solicitation or contract and the determination of whether to provide GFE is usually made by the government program manager and contracting officer. For our audit purposes, we may use GFP and GFE interchangeably to explain the regulatory requirements.

According to the FAR and DFARS, the contracting officer is responsible for including appropriate GFP contract clauses and preparing GFP listings in solicitations and awards as well as maintaining the listings in the contract throughout the performance period. For property accountability purposes, DoD Instruction requires accountability of GFP by contract number in the accountable property system of record.

RESULTS AND RECOMMENDATIONS

ACCOUNTABILITY OF GFE

We reviewed 17 contracts self-identified as containing GFE from three selected Acquisition Offices and determined DLA did not properly account for GFE provided to contractors. Specifically, Acquisition personnel did not properly identify GFE and maintain GFE listings within a contract. In addition, GFE was not easily traceable from the contract to EBS for accountability purposes. This occurred because contracting actions did not comply with FAR and DFARS requirements and DLA procedures to identify and account for GFE were not clearly defined. As a result, contracts did not properly identify the property offered to the contractor or changes to the actual property received. Additionally DLA was unable to identify a definitive population of contracts providing GFE and ensure proper accountability of equipment in EBS. This should be of concern to DLA because EBS information supports DLA's financial statements.

Contract Compliance and Property Accountability

To determine whether DLA properly accounted for GFE provided to contractors, our audit focused on contract compliance with preparing and maintaining GFE listings according to FAR and DFARS requirements and the EBS accountability of GFE listed in those contracts. During our audit, we worked with DLA Acquisition, DLA Installation Support, and DLA Information Operations personnel to identify a total population of DLA issued contracts that provided GFE to contactors; however, we were not able to identify a reliable contract population. Therefore, we coordinated with Acquisition personnel from DLA Energy, DLA Distribution, and DLA Contract Services Offices Ft Belvoir, VA and Columbus, OH, to self-identify DLA issued contracts that provided GFE to contactors. Of these self-identified contracts, we selected 17 contracts for review. The results of our review are detailed in the sections below.

Contract Compliance. Acquisition personnel did not properly identify GFE and maintain GFE listings within the contracts we reviewed for this audit. In order for a contract with GFE to be compliant, DLA must meet elements of both the FAR and DFARS. Specifically, we noted:

- FAR Part 45.201 requires the contracting officer to insert a listing of Government Property to be offered in all solicitations where government property is anticipated. The listing should include specific data elements such as the item name, quantity, a statement whether the property is to be furnished in an "as is" condition, and acquisition cost.
- DFARS Procedure Guidance Instruction (PGI) 245.103-72, implemented April 2012, requires contracting officers to use a particular format in solicitations and awards to specify the required Government Property data elements.
- DFARS PGI 245.103-73, requires the contracting officer to maintain the GFE listings.

- FAR 45.106 and DFARS PGI 245.103-71 requires transfers of property from one contract to the next to be documented by a modification to both the gaining and losing contracts.

During the audit, we evaluated documentation and spoke with contracting officers for 17 contracts to determine whether GFE listings were in compliance with applicable FAR and DFARS requirements. Although we identified instances where criteria was not applicable or we could not determine compliance due to non-compliance in other areas, Acquisition personnel generally did not properly identify GFE and maintain GFE listings in accordance with the FAR and DFARS. Table 1 summarizes the non-compliance areas we identified for the 17 contracts reviewed.

Non-Compliance Areas by Contract (Table 1)

Acquisition Office	Contract Number	GFE Listing with Required Data Elements (FAR Part 45.201)	Mandatory Reporting Format Effective April 2012 (DFARS PGI 245.103-72)	Contracting Officer Maintains GFE Listing (DFARS PGI 245.103-73)	Contract Modification to Transfer Property between Contracts (FAR 45.106)
DLA Energy	SP0600-11-C-5122	x	NA	Can't Determine	NA
	SP0600-14-C-5405	x	x	Can't Determine	NA
	SP0600-13-C-5348	x	x	Can't Determine	NA
	SP0600-13-C-5361	x	x	Compliant	NA
	SP0600-13-C-5347	x	x	x	NA
	SP0600-05-D-5500/ SP0600-13-C-5357	x	NA	Can't Determine	x
	SP0600-08-C-5832/ SP0600-13-C-5322	x	NA	Can't Determine	x
DLA Distribution	SP3300-10-C-0037	x	NA	x	NA
	SP3300-12-C-5001	x	x	x	NA
	SP3300-10-C-0006	x	NA	x	NA
	SP3300-13-C-0029	x	x	Compliant	NA
	SP3300-14-C-5003	x	x	x	NA
	SP3100-08-C-0001/ SP3300-12-C-5003	x	NA	Can’t Determine	x
	SP3300-11-C-0005	x	NA	Can't Determine	NA
DLA Contracting Services Office	SP4705-11-D-0001	x	NA	x	NA
	SP4706-13-C-0001	NA	NA	NA	NA
	SP4705-14-F0025	x	x	x	NA
Total Areas of Non-Compliance (x)	17 Contracts Reviewed	16	8	7	3

As the table indicates, 16 of the 17 contracts we reviewed were not in complete compliance with the FAR and DFARS requirements for GFE. In addition, we determined one contract, SP4706-13-C-0001, should not have been part of our GFE contract population because GFE was not provided to the contractor. This should be of particular concern to DLA Acquisition because contracting personnel were not aware which contracts provide GFE.

Property Accountability. GFE was not easily traceable from the contract to EBS for accountability purposes. According to DoD Instruction 5000.64, DoD components must use the accountable property system of record to account for GFP regardless of dollar value. Additionally, DoD Instruction 4161.02 requires DoD components to associate the contract number with GFP in the accountable property system of record. DLA implemented these requirements through two separate DLA Instructions. Specifically, DLA implemented the DoD Instruction 5000.64 through DLA Instruction 4202, Accountability and Management of DLA Equipment and other Accountable Property, and implemented DoD Instruction 4161.02 through DLA Instruction 4000.03, Accountability and Management of DLA-Owned Contract Property. However, DLA Instruction 4000.03 is only applicable to DLA Aviation, Land and Maritime, and Troop Support. Therefore, we only considered DLA Instruction 4202 when assessing property accountability during our audit. This instruction requires Accountable Property Officers (APO) to ensure all DLA property in the hands of a third party, including GFP, is accounted for in EBS.

During our audit, we spoke with the contracting officer and the APO or Accountable Property Manager for each contract we reviewed to understand how GFE traces from the contract to EBS for accountability purposes. We determined the contract number associated with GFE is not currently being entered in EBS as required by DoD Instruction 4161.02. Therefore, we could not reconcile the contracts we reviewed by contract number.

Because we could not reconcile the contracts by contract number, we also attempted an alternate reconciliation method during our audit. Specifically, we attempted to reconcile the contract GFE listings or the contractor transition inventory to the EBS site location active asset listing. Despite this procedure, we could only reconcile two of the 17 contracts with EBS and one contract was not applicable to our population.

Controls over GFE Accountability

DLA did not properly account for GFE provided to contractors because contracting actions did not comply with FAR and DFARS requirements and DLA procedures to identify and account for GFE were not clearly defined.

Acquisition Requirements. Acquisition personnel did not prepare and maintain the contract GFP listings according to FAR and DFARS requirements. Specifically, the GFE listings did not properly identify the GFE, reflect changes throughout the performance period, or include modifications at the end of a contract. For seven DLA Energy contracts, we determined the non-compliance was because there was not a common understanding of how to apply FAR Part 45 requirements for property incidental to the place of performance. Field Acquisition personnel explained FAR Part 45 requirements did not apply when the contract requires the contractor to perform work on a Government site or installation, and the property remains accountable to the

Government. However, General Counsel explained the FAR application of incidental to performance is situational-specific and therefore the FAR examples should be applied to each situation.

The FAR provides a series of examples of items that are considered incidental to the place of performance but, these examples are not all inclusive. The FAR examples include office space, desks, chairs, telephones, computers, and fax machines. The contracts we reviewed included incidental items as GFE, along with other items including vehicles, flow meter, gas generator, boat, and a portable oil boom. The other items were not aligned with the FAR examples and since all of these items were identified as GFE within the contract, the FAR and DFAR requirements should apply.

For the DLA Energy contracts, we noted an additional issue with the ownership of the property. DLA Energy explained the GFE on the contracts we reviewed contained Services-owned property and therefore was not accountable in EBS. However, for six contracts we were not able to clearly identify who owned the GFE, DLA or the Services. For three of those contracts, the GFE listings indicated that some of the property was owned by DLA. Clearly defining ownership of the property on the GFE listing promotes proper accountability for both DLA and the Military Services DLA supports.

As a result of the non-compliance, the contracts we reviewed did not properly identify the property offered to the contractor and contract modifications were not processed to reflect any changes to the actual property received. The contract establishes the legal authority to provide the property to the contractor and defines the responsibility for both the government and the contractor, including the authorization for the contractor to use the equipment. During our audit, DLA Acquisition took corrective action to provide Acquisition personnel guidance on Government Furnished Property regulations and instructions. Although the effectiveness of these actions have not been evaluated and may be subject to follow-up verification, the corrective actions taken were responsive to this issue. However, DLA Acquisition could continue to address this issue by coordinating with General Counsel to develop additional guidance for Contracting Officers clarifying how to decide which property is incidental to the contract, and which property should be classified as GFE, including Services-owned property. Further, DLA Acquisition should require Contracting Officers to clearly identify property ownership, whether DLA or Services-owned, on the GFE listing.

DLA Procedures. DLA procedures to identify and account for GFE were not clearly defined. We determined DLA does not have automated processes to identify all contracts that provide GFE to contractors and ensure proper accountability. Specifically, EBS asset listings did not include a specific contract number associated with items provided as GFE in order to identify an asset against a specific contract or to identify a population of contracts. According to DoD Instruction 4161.02, the contract number should be recorded in the accountable property system of record. EBS asset records contain a field designated for a contract number entry. However, we determined this field was not being populated with the contract number for our sample items and could not identify a DLA requirement to enter this information.

In addition, we could not identify any processes or procedures for Acquisition personnel to coordinate with the APO on GFE accountability in EBS. Although these two functions have different requirements, coordination is necessary in order to successfully account for the property. Specifically, the APO ensures GFP is accounted for in EBS while contracting officers prepare and maintain GFE listings according to FAR and DFARS requirements.

Without these procedures in place, DLA was unable to identify a definitive population of contracts providing GFE to contractors and ensure proper accountability of equipment in EBS, which should be of concern to DLA because EBS information supports DLA's financial statements. DLA should establish procedures for Acquisition personnel and APOs to coordinate on initial receipt and changes to GFE accountability in EBS throughout the contract performance period. These procedures should include establishing the contract number in the EBS asset record to associate the contract number with an asset provided as GFE to the contractor. This will result in a clear audit trail between the contract GFE listing and DLA property accounting records.

Recommendations for Director, DLA Acquisition (J7)

Recommendation 1. Coordinate with General Counsel to develop additional guidance for Contracting Officers clarifying how to decide which property is incidental to the contract, and which property should be classified as Government Furnished Equipment, including Services-owned property.

Management Comments. Concur. To address this recommendation, DLA J7 will issue a memorandum to the Heads of the Contracting Activities for DLA Aviation, DLA Energy, DLA Land & Maritime, DLA Troop Support, DLA Distribution, DLA Disposition Services, DLA Document Services, DLA Strategic Materials, and the DLA Contracting Support Office to include the importance of the need for contracting officers to coordinate with their cognizant Counsel Office to determine if property is incidental to the place of performance, on a case-by-case basis. The estimated completion date for corrective action is 30 days from the date of this audit report or July 10, 2015.

DLA OIG Response. Management comments were responsive to satisfy the intent of the recommendation.

Recommendation 2. Require Contracting Officers to provide clear identification of Government Furnished Equipment (GFE) ownership, whether DLA or Services-owned, on the GFE listing to ensure proper accountability.

Management Comments. Concur. To address this recommendation, DLA J7 will issue a memorandum (referenced in recommendation 1) to the Heads of the Contracting Activities for DLA Aviation, DLA Energy, DLA Land & Maritime, DLA Troop Support, DLA Distribution, DLA Disposition Services, DLA Document Services, DLA Strategic Materials, and the DLA Contracting Support Office to include the requirement for contracting officers to include GFE ownership in the award documents. The estimated completion date for corrective action is 30 days from the date of this audit report or July 10, 2015.

DLA OIG Response. Management comments were responsive to satisfy the intent of the recommendation.

Recommendation 3. Establish procedures for Contracting Officers when property is classified as Government Furnished Equipment (GFE), to provide pertinent contract information, including the contract number, to those responsible for maintaining Enterprise Business System asset records. The contract information should include the minimum amount of information necessary to identify and inventory a complete universe of GFE provided to contractors.

Management Comments. Concur. To address this recommendation, DLA J7 will issue a memorandum (referenced in recommendation 1) to the Heads of the Contracting Activities for DLA Aviation, DLA Energy, DLA Land & Maritime, DLA Troop Support, DLA Distribution, DLA Disposition Services, DLA Document Services, DLA Strategic Materials, and the DLA Contracting Support Office to include the requirement to establish procedures for contracting officers to provide pertinent contract information to those responsible for maintaining EBS asset records. The estimated completion date for corrective action is 30 days from the date of this audit report or July 10, 2015.

DLA OIG Response. Management comments were responsive to satisfy the intent of the recommendation.

Recommendation for Director, DLA Installation Support

Recommendation 4. Establish procedures for Accountable Property Officers to document pertinent contract information, including the contract number, in the Enterprise Business System (EBS) asset record to associate the contract number and other key contract information with the specific Government Furnished Equipment (GFE) provided to the contractor. The contract information in EBS should include the minimum amount of information necessary to identify and inventory a complete universe of GFE provided to contractors.

Management Comments. Concur. To address this recommendation, DLA Installation Support will review the current policy for gaps and draft additional guidance for implementation through a Directive Type Memorandum (DTM). Upon receipt from J7 of an executed contract, with GFE properly delineated, the contract number and other key contract information for the specific GFE provided to the contractor will be entered in EBS. DLA Installation Support will coordinate with J7 to ensure policies are in place to provide end-to-end procedures for tracking and accounting for GFE. During the next update, no later than second quarter FY16, DLA Installation Support will include the DTM language in the general equipment DLA Manual. The estimated completion date for the DTM corrective action is no later than 60 days from the date of this report or August 10, 2015.

DLA OIG Response. Management comments were responsive to satisfy the intent of the recommendation.

APPENDIX A. SCOPE AND METHODOLOGY

On July 8, 2014, the DLA OIG announced the Audit of Government-Furnished Equipment Provided to Contractors. We conducted this performance audit based on an internally developed topic included in the DLA OIG FY14/15 Audit and Crime Vulnerability Assessment Plan. Our audit objective was to determine whether DLA properly accounted for government furnished equipment provided to contractors.

We conducted fieldwork for this performance audit from September 2014 to April 2015 in accordance with generally accepted government auditing standards (GAGAS). 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To determine whether DLA properly accounted for government furnished equipment provided to contractors we conducted audit work at three DLA Acquisition Offices and

- Reviewed contract files for evidence of GFE,
- Interviewed contracting personnel and APO/managers,
- Reconciled contract GFE listings to the EBS site location active asset listing,
- Evaluated compliance with applicable criteria.

Population Identification. We met with DLA Acquisition personnel on multiple occasions to identify the population of contracts that provide GFE to contractors in order to evaluate our audit objective. DLA Acquisition confirmed there are no automated processes to identify these types of contracts. We identified the Federal Procurement Data System – Next Generation (FPDS-NG) as a possible source of information. However, we determined FPDS only identifies contracts with a GFP/GFE indicator. FPDS does not discriminate between the types of property provided and therefore, could not be used as a population source.

We also met with DLA Installation Support to determine if the accountable property system of record, EBS, could identify contracts that provide GFE. Unfortunately the EBS asset data for items Installation Support identified as GFE did not include a contract number associated with an asset line item.

In addition, we contacted DLA Information Operations - Procurement Requirements and Integration EBS Portfolio Management to determine if there was an indicator within the contract writing system to identify contracts that provide GFE. We determined there is a code for material, tooling, and property, but nothing specific to equipment. Therefore, the procurement module of EBS could not be used as a population source.

Site Selection Process. To answer our audit objective, we judgmentally selected three locations to evaluate how DLA accounts for GFE across the agency. Since DLA does not have an automated process to identify the population of GFE contracts, we considered the following two factors when selecting locations:

- The number of contracts identified with a GFP/GFE indicator in the Federal Procurement Data System – Next Generation from the time period October 1, 2000 through September 8, 2014.
- The potential identified contracts included GFE rather than government furnished material.

Based on these selection factors, we selected and reviewed GFE accountability procedures at DLA Energy, DLA Distribution and DLA Contracting Services Office (DCSO) because those locations had the highest potential for contracts containing GFE.

Contract Selection Process. To evaluate how the three selected locations account for GFE, we judgmentally selected contracts for review from a population of self-identified contracts provided to us. Specifically, the three DLA Acquisition Offices self-reported contracts that provided GFE and met the following criteria:

- Open contracts as of September 1, 2014.
- Contracts where the performance period ended during the time August 31, 2012 through September 1, 2014.

From the self-identified list, we considered the following two factors when selecting contracts:

- The contracts did not show an indicator of GFP/GFE in FPDS.
- The contracts provided a variety of GFE.

Based on these factors, we selected 10 open contracts and four where the performance period had ended from the self-reported list of contracts at DLA Energy and DLA Distribution. We also reviewed the follow-on contract, if applicable, for those contracts where the performance period ended. We determined DCSO did not provide the proper information in order to identify the population of contracts. DCSO provided a FPDS data pull which we previously determined was not an adequate source for population identification. As an alternative, we requested DCSO contracts at Ft. Belvoir and Columbus to review. DCSO Ft. Belvoir provided three applicable contracts for review. However, we were not able to complete audit fieldwork at DCSO Columbus because the requested contract information was not provided to us for review and analysis during audit fieldwork. As a result, we selected and reviewed GFE accountability for 17 contracts because we wanted to review procedures across multiple DLA locations. The results of our audit cannot be projected across the population at an individual site or DLA Acquisition as a whole. Table 2 summarizes the contracts we reviewed at each acquisition office.

Self-Reported and Reviewed Contracts (Table 2)					
Acquisition Office	Total Contracts Self-Reported - Ongoing Performance as of 1 Sep 2014	Contracts Reviewed - Ongoing Performance as of 1 Sept 2014	Total Contracts Self-Reported-Performance Ended From 31 Aug 2012 – 1 Sept 2014	Contracts Reviewed - Performance Ended from 31 Aug 2012 - 1 Sept 2014	Total Reviewed
DLA Energy	80	5	39	2	7
DLA Distribution	11	5	6	2	7
DCSO Ft. Belvoir and Columbus	Didn't provide an accurate population	3	Didn't provide requested data	0	3
Total	Can't determine	13	Can't determine	4	17

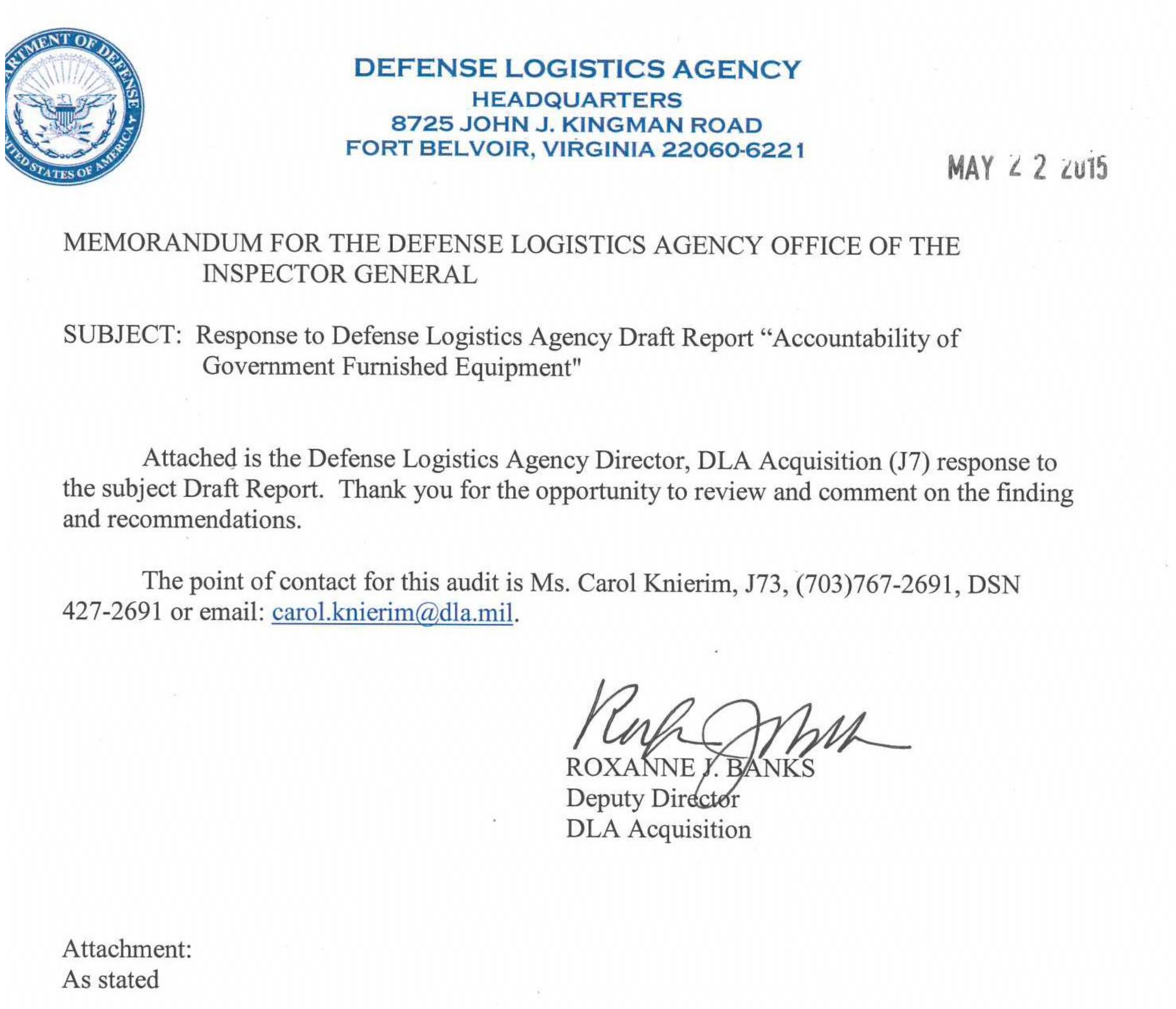
Data Reliability. We used information from various sources during our audit. The extent and usage of the information is explained below.

- Federal Procurement Data System – Next Generation. We did not assess the reliability of data extracted from FPDS because it did not materially affect our findings, conclusions, or recommendations. We used the data as background information and a factor in judgmentally selecting our sites and in some instances selecting contracts for review.

- Self-reported contracts. We relied on the three Acquisition Offices to provide complete and accurate reporting of the contracts. Since DLA does not have an automated process to report the contracts that provide GFE, there was no other corroborating evidence or alternative procedures for us to verify the accuracy of the contracts reported.

- Enterprise Business System. To assess the reliability of data extracted from the EBS we met with APO and DLA Installation Support to verify the contract number is an available field to populate in EBS and that no current procedures exist to add this information to an asset line item. We also used the EBS site location active asset list generated by the APO to compare with the contract GFE listings or transition inventory. We did not conduct tests to determine the information contained in those reports was accurate; however, we compared the information to the contract GFE listings and spoke with contracting personnel and APO and managers to reach our audit conclusions. As a result, the risks associated with using the computer processed data from EBS were mitigated and did not impact answering our audit objective.

APPENDIX B. MANAGEMENT COMMENTS



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

MAY 22 2015

MEMORANDUM FOR THE DEFENSE LOGISTICS AGENCY OFFICE OF THE INSPECTOR GENERAL

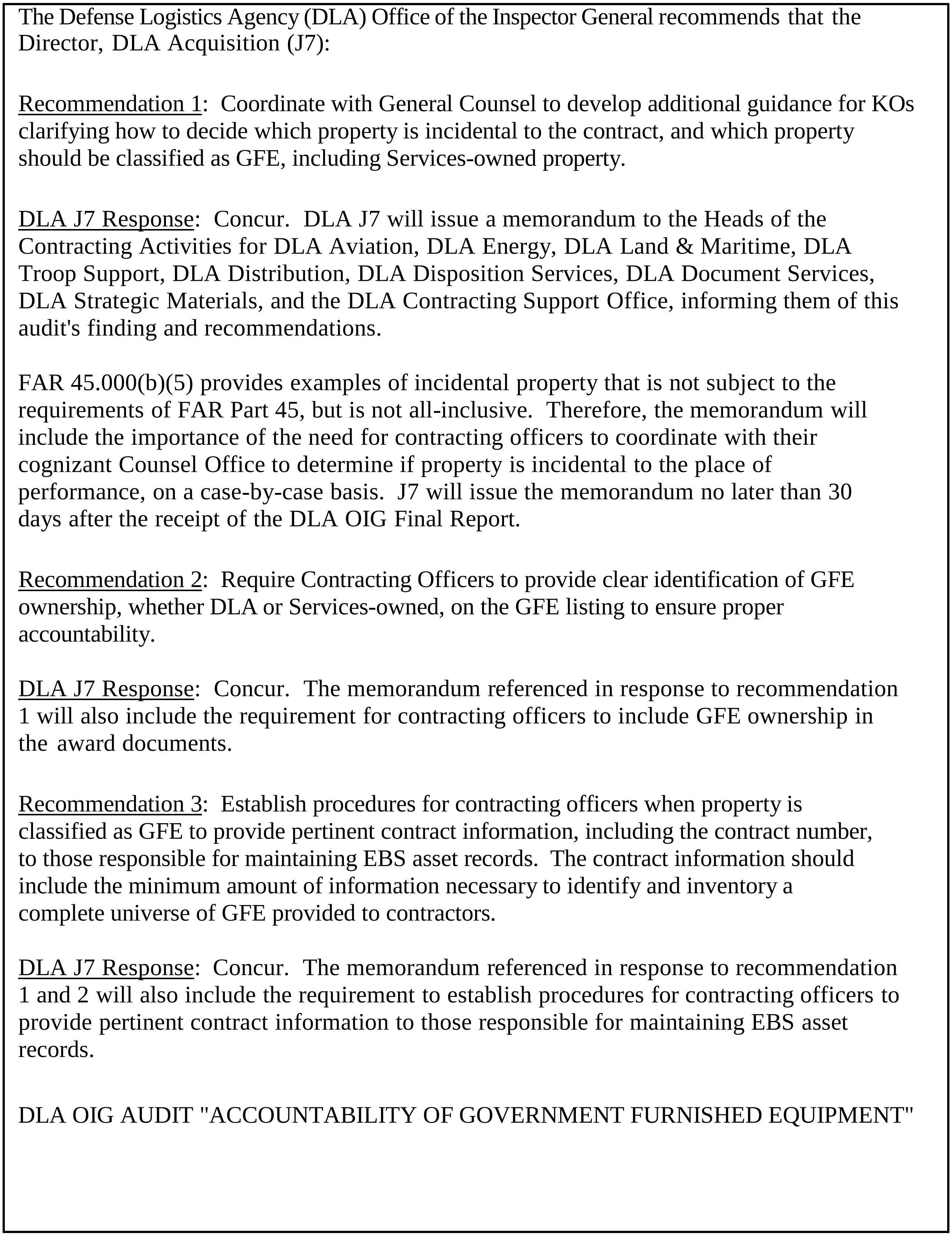
SUBJECT: Response to Defense Logistics Agency Draft Report "Accountability of Government Furnished Equipment"

Attached is the Defense Logistics Agency Director, DLA Acquisition (J7) response to the subject Draft Report. Thank you for the opportunity to review and comment on the finding and recommendations.

The point of contact for this audit is Ms. Carol Knierim, J73, (703)767-2691, DSN 427-2691 or email: carol.knierim@dla.mil.

ROXANNE J. BANKS
Deputy Director
DLA Acquisition

Attachment:
As stated



The Defense Logistics Agency (DLA) Office of the Inspector General recommends that the Director, DLA Acquisition (J7):

Recommendation 1: Coordinate with General Counsel to develop additional guidance for KOs clarifying how to decide which property is incidental to the contract, and which property should be classified as GFE, including Services-owned property.

DLA J7 Response: Concur. DLA J7 will issue a memorandum to the Heads of the Contracting Activities for DLA Aviation, DLA Energy, DLA Land & Maritime, DLA Troop Support, DLA Distribution, DLA Disposition Services, DLA Document Services, DLA Strategic Materials, and the DLA Contracting Support Office, informing them of this audit's finding and recommendations.

FAR 45.000(b)(5) provides examples of incidental property that is not subject to the requirements of FAR Part 45, but is not all-inclusive. Therefore, the memorandum will include the importance of the need for contracting officers to coordinate with their cognizant Counsel Office to determine if property is incidental to the place of performance, on a case-by-case basis. J7 will issue the memorandum no later than 30 days after the receipt of the DLA OIG Final Report.

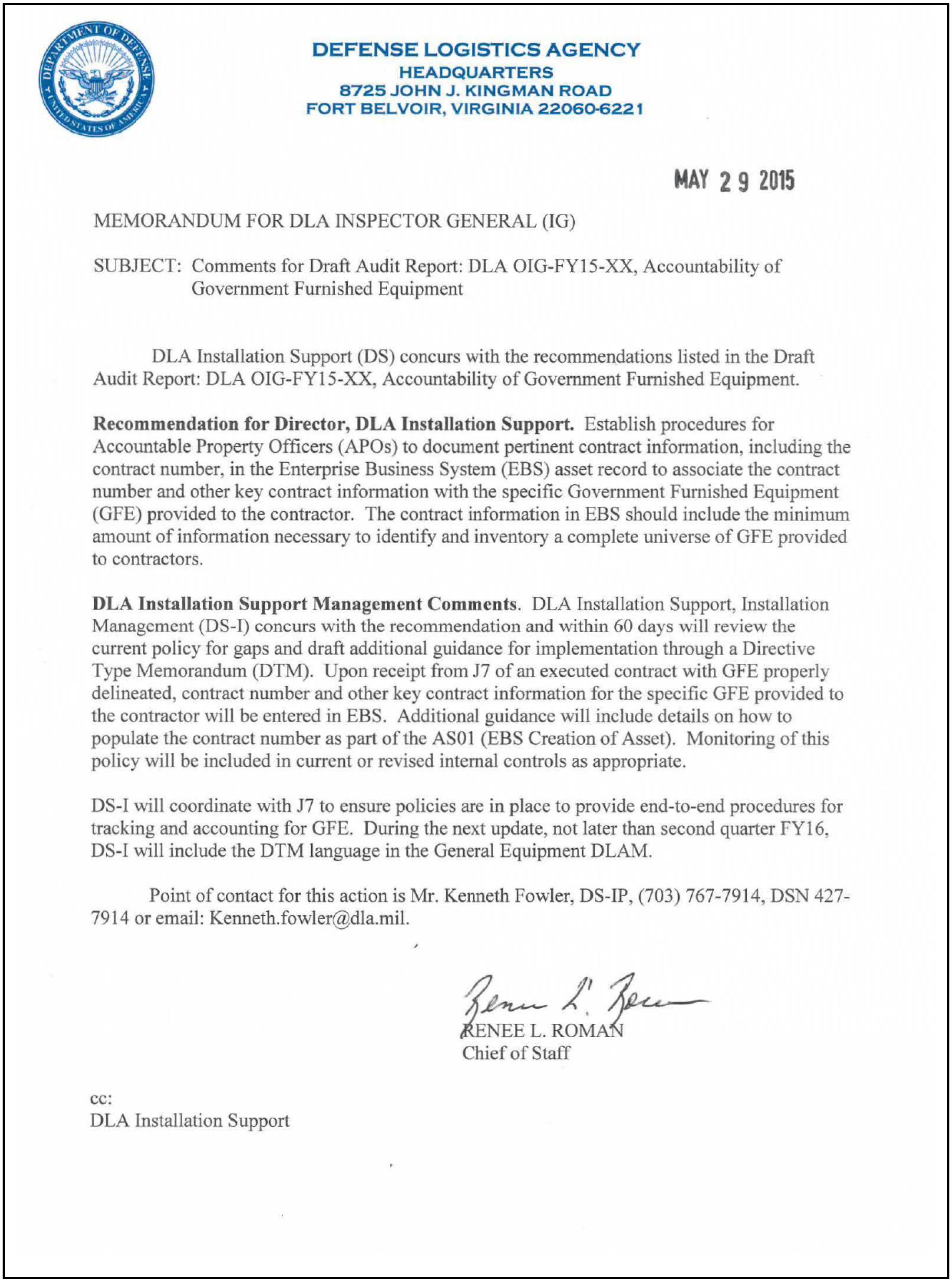
Recommendation 2: Require Contracting Officers to provide clear identification of GFE ownership, whether DLA or Services-owned, on the GFE listing to ensure proper accountability.

DLA J7 Response: Concur. The memorandum referenced in response to recommendation 1 will also include the requirement for contracting officers to include GFE ownership in the award documents.

Recommendation 3: Establish procedures for contracting officers when property is classified as GFE to provide pertinent contract information, including the contract number, to those responsible for maintaining EBS asset records. The contract information should include the minimum amount of information necessary to identify and inventory a complete universe of GFE provided to contractors.

DLA J7 Response: Concur. The memorandum referenced in response to recommendation 1 and 2 will also include the requirement to establish procedures for contracting officers to provide pertinent contract information to those responsible for maintaining EBS asset records.

DLA OIG AUDIT "ACCOUNTABILITY OF GOVERNMENT FURNISHED EQUIPMENT"



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

MAY 29 2015

MEMORANDUM FOR DLA INSPECTOR GENERAL (IG)

SUBJECT: Comments for Draft Audit Report: DLA OIG-FY15-XX, Accountability of Government Furnished Equipment

DLA Installation Support (DS) concurs with the recommendations listed in the Draft Audit Report: DLA OIG-FY15-XX, Accountability of Government Furnished Equipment.

Recommendation for Director, DLA Installation Support. Establish procedures for Accountable Property Officers (APOs) to document pertinent contract information, including the contract number, in the Enterprise Business System (EBS) asset record to associate the contract number and other key contract information with the specific Government Furnished Equipment (GFE) provided to the contractor. The contract information in EBS should include the minimum amount of information necessary to identify and inventory a complete universe of GFE provided to contractors.

DLA Installation Support Management Comments. DLA Installation Support, Installation Management (DS-I) concurs with the recommendation and within 60 days will review the current policy for gaps and draft additional guidance for implementation through a Directive Type Memorandum (DTM). Upon receipt from J7 of an executed contract with GFE properly delineated, contract number and other key contract information for the specific GFE provided to the contractor will be entered in EBS. Additional guidance will include details on how to populate the contract number as part of the AS01 (EBS Creation of Asset). Monitoring of this policy will be included in current or revised internal controls as appropriate.

DS-I will coordinate with J7 to ensure policies are in place to provide end-to-end procedures for tracking and accounting for GFE. During the next update, not later than second quarter FY16, DS-I will include the DTM language in the General Equipment DLAM.

Point of contact for this action is Mr. Kenneth Fowler, DS-IP, (703) 767-7914, DSN 427-7914 or email: Kenneth.fowler@dla.mil.

RENEE L. ROMAN
Chief of Staff

cc:
DLA Installation Support

DLA Office of the Inspector General

Sole Source Service Contracts

Audit Report: DLA OIG-FY15-07 **September 25, 2015**

MISSION

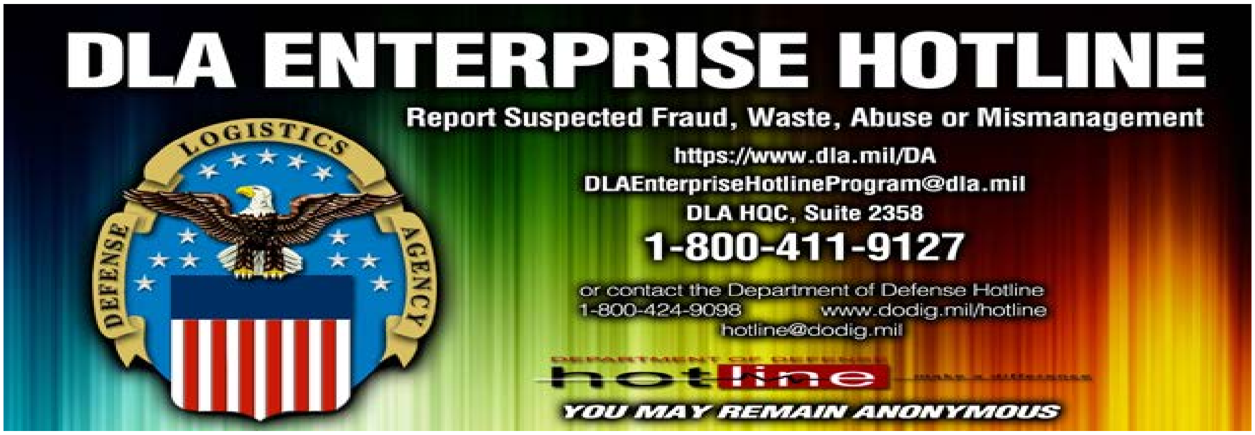
The DLA Office of the Inspector General Audit Division provides DLA leadership with sound advice and recommendations to assist them in making informed decisions to improve support to the warfighter, and proper stewardship of resources while remaining independent and objective in our auditing approach.

VISION

Motivated and trusted audit professionals who provide timely and value-added audit services emphasizing collaboration with management, risk mitigation and accountability.

Suggestion for Audits

To suggest or request audits, contact the office of the Deputy Inspector General for Auditing at OIG_Audit@dla.mil.



DLA ENTERPRISE HOTLINE

Report Suspected Fraud, Waste, Abuse or Mismanagement

https://www.dla.mil/DA
DLAEnterpriseHotlineProgram@dla.mil
DLA HQC, Suite 2358
1-800-411-9127

or contact the Department of Defense Hotline
1-800-424-9098 www.dodig.mil/hotline
hotline@dodig.mil

DEPARTMENT OF DEFENSE
hotline

YOU MAY REMAIN ANONYMOUS

Acronyms Used

J&A	Justification and Approval
FAR	Federal Acquisition Regulation
FedBizOps	Federal Business Opportunities
GAO	Government Accountability Office
DoDIG	Department of Defense Office of the Inspector General
ILS	Inventory Locator Service
FPDS-NG	Federal Procurement Data System - Next Generation
DCSO	DLA Contract Services Office

Report No. DLAOIG-FY15-07 (Project No. FY15-DLAOIG-05) September 25, 2015

Executive Summary: Sole Source Service Contracts

What We Did and Why

The objective of our audit was to determine whether DLA Acquisition (J7) and DLA Energy had proper justifications, support, and approvals for sole source service contracts awarded in 2013 and 2014. Our audit was initiated as part of the DLA FY 2014 Audit and Crime Vulnerability Assessment Plan dated December 19, 2013. This plan identified the collection of vendor performance data as a potential audit topic. However, the focus of our audit changed to sole source service contracts during the audit planning phase after the audit team performed a risk assessment identifying that recent DoDIG procurement audits did not examine sole source justifications and approvals for service contracts. As a result, we focused our audit on sole source service contracts to provide DLA Acquisition a holistic view of sole source contracting.

What We Found

Generally, DLA Acquisition’s (J7) Contract Services Office and DLA Energy contracting personnel maintained proper justifications, support, and approvals for sole source service contracts awarded in 2013 and 2014. As a result, DLA Acquisition’s (J7) Contract Services Office and DLA Energy contracting personnel justified the use of other than full and open competition for six of eight contracts reviewed.

Although we identified a few instances where contracting officials deviated from the justification and approval process, each contracting office had internal controls in place to prevent these mistakes. These internal controls include: (1) adherence to FAR directives for justification and approval documents, (2) review by DLA General Counsel of all justification and approval documents for procurements over $150,000, and (3) appointing a competition advocate for each contracting element.

What We Recommend

Although we found that a DLA Energy contracting official made an error by not preparing a justification and approval document for one contract; and the contracting officials in DLA Acquisition’s (J7) Contract Services Office did not make justification and approval documents publicly available, or properly justify one sole source contract, we did not find that these omissions were systemic. Therefore, we are not making any recommendations.

Management Comments and Our Response

Since this report contained no recommendations, management comments were not required. However, DLA Acquisition J7 did summit official comments and we included those verbatim comments in Appendix B of this report.

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

September 25, 2015

MEMORANDUM FOR DIRECTOR, DLA ACQUISITION (J7) AND COMMANDER, DLA ENERGY

SUBJECT: Final Report: Audit of Sole Source Service Contracts, Report No. DLA OIG-FY15-07 (Project No. FY15-DLAOIG-05)

This is the final report on the Audit of Sole Source Service Contracts. This report contains no recommendations.

The objective of our audit was to determine whether DLA Acquisition (J7) and DLA Energy had proper justifications, support, and approvals (J&As) for sole source service contracts awarded in 2013 and 2014.

DLA Acquisition's Contract Services Office (DSCO) and DLA Energy contracting personnel generally met FAR requirements for justifying, supporting and approving J&As. However due to oversight, time constraints and heavy workload, contracting officials did make some errors in the J&A process.

Although we identified deficiencies where contracting officers deviated from the justification and approval process, each contracting office had internal controls in place to prevent these deficiencies. These internal controls include: (1) adherence to FAR directives for justification and approval documents, (2) review by DLA General Counsel of all justification and approval documents for procurements over $150,000, and (3) appointing a competition advocate for each contracting element. We did not consider the identified deficiencies as systemic problems and, therefore, did not issue any recommendations as result of our audit.

Since this report contained no recommendations, management comments were not required. However, J7 did summit official comments and we included those verbatim comments in Appendix B of this report.

We appreciate the courtesies and cooperation extended to us during the audit. For additional information about this report please contact Ms. Tamonie Denegall at 703-767-6263 or email at tamonie.denegall@dla.mil.

Steven D Pigott

STEVEN D. PIGOTT
Deputy Inspector General
DLA OIG Audit Division

CONTENTS

Introduction

Appendices

DEVELOPMENT OF THE AUDIT

Our audit was initiated as part of the DLA FY 2014 Audit and Crime Vulnerability Assessment Plan dated December 19, 2013. This plan identified the collection of vendor performance data as a potential audit topic. However, the focus of our audit changed to sole source service contracts as a result of our risk assessment which identified that recent DoDIG procurement audits did not examine sole source justification and approvals (J&As) for service contracts. As a result, we focused our audit on sole source service contacts to provide DLA Acquisition a holistic view of sole source service contracting. Our audit was subsequently included in the approved DLA FY15-FY16 Audit Plan as the "Sole Source Service Contracts Audit."

While conducting this audit, we focused on DLA Acquisition's (J7) Contracting Services Office (DCSO) and DLA Energy contracting actions and obtained an understanding of the audit area by reviewing the annual statements of assurance, managers internal control documentation, and previous audit work. We focused on these two offices because according to the FPDS-NG data, DLA Energy, DLA Aviation and DLA Troop Support issued the majority of sole source contracts.

Annual Statements of Assurance

DLA Acquisition (J7) annual statements of assurance for FY2013 and FY2014 did not identify sole source service contracts as a high risk or note any material weaknesses related to our audit area. To determine high risk areas and whether material weaknesses exist in acquisition processes, DLA Acquisition used the Procurement Management Review (PMR) process as its primary internal control assessment tool. DLA Acquisition used this tool to provide monitoring and oversight for the contracting and procurement function across the enterprise.

Managers Internal Controls

DCSO and DLA Energy had controls in place to make sure sole source service contracts had proper justifications and approvals. These internal controls include: (1) adherence to FAR directives for justification and approval documents, (2) review by DLA General Counsel of all justification and approval documents for procurements over $150,000, and (3) appointing a competition advocate for each contracting element.

Previous Audit Work

The procurement process is part of the Procure-to-Pay business cycle. At the time of this audit, DLA Finance (J8) had made no assertions in regards to the procure-to-pay business cycle. While planning our audit, we identified that DoDIG conducted audit work related to sole source contracts in DODIG-2014-088 "Defense Logistics Agency Aviation Potentially Overpaid Bell Helicopter for Sole-Source Commercial Spare Parts" dated July 7, 2014, and DODIG-2014-110 "Ontic Engineering and Manufacturing Overcharged the Defense Logistics Agency for Sole-Source Spare Part" dated September 15, 2014. Although these audits did not include sole source service contracts, we reviewed these audit reports to understand the DoDIG's audit approach.

Prior to this audit, the DLA OIG had not performed audit work related to sole source contracts.

OBJECTIVE AND CONCLUSION

The objective of our audit was to determine whether DLA Acquisition (J7) and DLA Energy had proper justifications, support, and approvals for sole source service contracts awarded in 2013 and 2014.

DLA Acquisition's (J7) DCSO and DLA Energy contracting personnel generally met FAR requirements for justifying, supporting and approving J&As. However due to oversight, time constraints and heavy workload, contracting officials did make some errors in the J&A process.

Although we identified deficiencies where contracting officers deviated from the justification and approval process, each contracting office had internal controls in place to prevent these deficiencies. These internal controls include: (1) adherence to FAR directives for justification and approval documents, (2) review by DLA General Counsel of all justification and approval documents for procurements over $150,000, and (3) appointing a competition advocate for each contracting element. We did not consider the identified deficiencies as systemic problems and, therefore, did not issue any recommendations as result of our audit.

BACKGROUND

Full and open competition is the preferred method for Federal agencies to award contracts. Section 2304, title 10 of the United States Code requires contracting officers, with certain exceptions, to promote and provide for full and open competition when soliciting offers and awarding contracts.

A sole-source contract is a contract that is entered into or proposed to be entered into by an agency after soliciting and negotiating with only one source or vendor. With limited exceptions, a sole-source contract requires a J&A. The vision of the Federal Acquisition System (FAS), as established in the Federal Acquisition Regulation (FAR), is to deliver on a timely basis the best value product or service to the customer, while maintaining the public's trust and fulfilling public policy objectives. Best value means that the expected outcome of the acquisition provides the greatest overall benefit in response to the government's requirements. Best value must be viewed from a broad perspective and is achieved by balancing competing interests in the FAS. One way the government expects to achieve best value is through competition. Further, FAS' policy is to promote competition in the acquisition process. Therefore, an agency's decision to limit competition in contracting should be carefully considered.

Contracting officers may use procedures other than full and open competition under certain circumstances; however, each contract awarded without providing for full and open competition must follow FAR Subpart 6.3, "Other Than Full and Open Competition." FAR 6.3 established the policies and procedures and identify the statutory authorities for contracting without full and open competition to include conducting market research and making J&As publicly available in Federal Business Opportunities (FedBizOps).

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 that programs are operating as intended and to evaluate the effectiveness of controls. Internal controls—organization, policies, and procedures—are tools to help program and financial managers achieve results and safeguard the integrity of their programs. During the course of our audit, we reviewed supporting J&A documentation for eight sole source service contracts. We found two instances where contracting personnel deviated from the J&A process. However, we found DCSO and DLA Energy had internal controls in place to prevent and detect errors for sole source service justification and approval documents, and we discuss these controls in the Internal Controls section on page eight of this report. Although we did not identify an internal control deficiency as a result of our audit work, the scope of work did not include all sole source contracts and DCSO and DLA Energy remain responsible for maintaining effective internal controls to ensure sole source contracts are processed appropriately.

RESULTS AND RECOMMENDATIONS

Generally, J7's DCSO and DLA Energy contracting personnel maintained proper justifications, support, and approvals for sole source service contracts awarded in FY2013 and FY2014. DCSO and DLA Energy contracting personnel properly justified the use of other than full and open competition for six of eight contracts. This occurred because each contacting office had internal controls in place to make sure J&As met FAR requirements for awarding contracts using other than full and open competition. However, the contracting officials deviated from the J&A process for two of the eight contracts.

SOLE SOURCE SERVICE CONTRACTS

During our audit, we identified 44 DLA sole source service contracts, valued at approximately $93.4 million that were classified as "Not Competed" during FY2013 and FY2014. Of these 44 DLA contracts, we identified 32 sole source services contracts valued at approximately $67.7 million, and selected a non-statistical sample of eight contracts valued at $16 million for review. We excluded the remaining 12 contracts because they were for information technology services, which DODIG recently reviewed. We determined DSCO and DLA Energy contracting personnel justified the use of other than full and open competition for six of eight contracts. For the six contracts, DSCO and DLA Energy contracting personnel generally:

- Complied with FAR 6.303-2, "Content," requirements in the J&As,
- Appropriately applied the authority cited,
- Obtained approval from the proper personnel before contract award,
- Documented compliance with FAR Part 10, "Market Research" and,
- Complied with FAR 6.305 "Availability of the Justification".

However, the contracting officials deviated from the J&A process for two of the eight contracts. Specifically, DLA Energy did not prepare a J&A for one of its contract actions and DCSO did not sufficiently justify the use of the specific authority cited for one contract. Also, DCSO contracting officials did not always make the J&As publicly available.

We discuss our findings in detail in the following sections.

DLA Energy

DLA Energy contracting officers generally maintained proper justifications, support, and approvals for sole source service contracts. FAR 6.3 "Other Than Full and Open Competition" prescribe policies and procedures for contracting without providing for full and open competition. Table 1 summarizes the four DLA Energy contracts we reviewed, and identifies where contracting officials deviated from the J&A process.

Table 1: Summary of DLA Energy Non-compliances

Contract Number	Contract Action	Contractor Name	FAR 6.303 Justification	FAR 6.304 Approval	FAR 6.305 Availability
SP0600-13-D-5354	Base	Shaw			
SP0600-13-C-9304	Base	Platts			
SP0600-14-C-5407	Base	Cogeco			
	Option	Cogeco			
	Extension	Cogeco			
SPE600-14-D-0451	Base	Western Container	x	x	x

X = Indicates non-compliance identified

Although DLA Energy followed the J&A process for three contracts, we identified some deficiencies with the SPE600-14-D-0451 contract.

Contract SPE600-14-D-0451 is a service contract for the storage and transportation of DOD Leased Bulk Fuel Containers issued to Western Container Transport. DLA Energy's contracting office initially awarded the contract for an amount under the simplified acquisition threshold of $150,000. Subsequently, contracting officials modified the contract and increased the value which exceeded the simplified acquisition threshold without preparing a J&A. The contracting personnel told us this occurred because of the change in personnel and the shifting of workload.

DLA Contract Service Office

DCSO contracting officers generally maintained proper justifications, support, and approvals for three out of four sole source service contracts we reviewed. FAR 6.3 "Other Than Full and Open Competition" prescribe policies and procedures for contracting without providing for full and open competition. Table 2 summarizes the results of our view of the J&As on the four DCSO contracts we reviewed, and identifies where contracting officials deviated from the J&A process.

Table 2: Summary of DCSO Non-compliances

Contract Number	Contract Action	Contractor Name	FAR 6.303 Justification	FAR 6.304 Approval	FAR 6.305 Availability
SP4705-14-C-0032	Base	Crowley			X – late
SP4705-14-C-0033	Base	Crowley			X – late
SP4703-13-C-5024	Base	ILS	X		X
SP4703-13-C-0018	Base	Eyak			
	Option	Eyak			X
	Extension	Eyak			X

X = Indicates non-compliance identified

Although DCSO generally followed the J&A process for three contracts, we identified some deficiencies with the SP4703-13-C-5024 contract.

Contract SP4703-13-C-5024, is a service contract that provides Inventory Locator Service (ILS) support. DCSO contracting officials did not make sure that the J&A:

- Contained sufficient facts and rationale to justify the use of the specific authority cited as required by FAR 6.303-2(a) and,
- Was made publicly available by posting to FedBizOps.

According to contracting officials, these errors occurred because of time constraints.

On the other three contracts we reviewed, we found that contracting officials posted late or did not make the J&As publicly available on FedBizOps as required by FAR subpart 6.305. Contracting officials attributed the errors to oversight and heavy workload.

INTERNAL CONTROLS

DLA Energy and DCSO generally documented J&As for sole source service contact in accordance with the FAR because the contracting offices had internal controls in place to prevent deficiencies.

Although DLA Energy and DCSO contracting officials made the errors cited above, we did not find these errors to be systemic issues. The contracting offices had internal controls in place to prevent these errors from occurring. These internal controls include: (1) adherence to FAR directives for justification and approval documents, (2) review by DLA General Counsel of all justification and approval documents for procurements over $150,000, and (3) appointing a competition advocate for each contracting element.

Additionally, DLA Energy contracting officials have taken steps to strengthen controls to help mitigate the risks associated with awarding sole source contracts. The contract office issued Contracting Instruction (CI) 15-08 dated October 9, 2014, "Justification and Approval (J&A) Tracking Log and Procedures." The instruction requires all J&As, including those approved at the contracting officer level, be entered into a log and have a tracking number assigned. This instruction will help the contracting officers make sure J&As are reviewed and approved by the required authority before the contract is awarded. Additionally, contracting officials took additional steps to develop a Justification and Approval (J&A) Template and Routing Procedures CI 15-29 dated February 24, 2015. This instruction serves as another aid to help contracting officers meet FAR requirements for preparing, supporting and approving J&As.

DCSO has pre- and post-award contract checklists in place that serve as a reminder of the FAR requirements. As a result of these controls, we did not find these deficiencies to be systemic and therefore, we will not make any recommendations based on our audit.

APPENDIX A. SCOPE AND METHODOLOGY

On February 26, 2015 the DLA OIG announced the Audit of Sole Source Service Contracts. We conducted fieldwork for this performance audit based on a topic included in the DLA OIG FY2014/15 Audit and Crime Vulnerability Assessment Plan. The decision to focus on sole source service contracts was due to the audit coverage provided by DoDIG on supply and information technology sole source contracts.

We conducted fieldwork for this performance audit from March 26, 2015 to July 6, 2015 in accordance with generally accepted government auditing standards (GAGAS). 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To determine whether DLA Acquisition (J7) and DLA Energy had proper justifications, support, and approvals for sole source service contracts awarded in FY2013 and FY2014, we:

1. Obtained and reviewed the following guidance:
    - Section 2304, title 10 of the United Sates Code,
    - FAR Subpart 6.3, “Other Than Full and Open Competition”,
    - FAR part 5 “Publicizing Contract Actions”,
    - FAR part 10, “Market Research”, and
    - Defense Logistics Acquisition Directive, Revision 5, August 22, 2014.

2. Interviewed and obtained contract records from personnel in DLA Acquisition (J7), DLA Energy, and DCSO in Ft. Belvoir, Richmond, VA, and Philadelphia, PA.

3. Interviewed Competition Advocates in DLA Acquisition (J7), DLA Energy, and DCSO to gain an understanding of their role in the sole source process.

4. Interviewed General Counsel to identify what elements they review when approving a J&A.

5. Reviewed the FY2013 and FY2014 Statements of Assurance for DLA, DLA Energy and DLA Acquisition to determine if sole source service contracts had been identified as a high risk area; and whether material weakness had been identified and reported. Interviewed the management internal control administrator for each activity.

6. Reviewed the following contracts:
    - SP4705-14-C-0032 , Crowley Logistics, Charting a foreign flagged vessel,
    - SP4705-14-C-0033, Crowley Logistics, Operation/Management of warehouse,
    - SP4703-13-C-5024, Inventory Locator Service, ILS Software maintenance,
    - SP4701-13-C-0018, EYAK Technology, Help Desk Support,
    - SP0600-14-C-5407, Cogeco Private Limited, Inspection of tanks and trucks,

- SP0600-13-D-5354, Shaw Environmental, Remediation Services,
- SP0600-13-C-9304, Platts, Annual Subscription Renewal, and
- SPE600-14-D-0451, Western Container, Storage and Transport of Bulk Fuel Containers.

SCOPE

We used the Federal Procurement Data System – Next Generation (FPDS-NG) to establish the universe of sole source service contracts for this audit. In prior GAO reports, GAO documented that FPDS-NG often contains inaccurate data. So, we performed additional audit procedures such as obtaining the J&A log from DCSO and a list of sole source contract numbers from DLA Energy -- to provide some assurance that we had obtained a complete universe of sole source service contracts.

According to the FPDS-NG data, DLA Energy, DLA Aviation and DLA Troop Support had the majority of sole source contracts. DLA Energy maintains its own contracting elements to service its unique mission to provide DoD and other government agencies with comprehensive energy solutions. At DLA Aviation and DLA Troop Support, DCSO has responsibility for full life-cycle contracting process for a variety of highly specialized areas such as IT, research and development, logistics, contractor support, consultants, facilities maintenance and financial services and associated supplies in support of DLA internal operations and other supported activities. As a result, we developed a non-statistical sample of DLA Energy and DCSO sole source service contracts executed for DLA Aviation and DLA Troop Support based on analyzing the FY2013 and FY 2014 FPDS-NG "Not Competed" data. The audit team excluded IT contracts from our sample because DoDIG had announced an audit covering sole source IT contracts. We also excluded any contracts below the simplified acquisition threshold of $150,000, and small business set asides. We selected three DLA Energy contracts and three DCSO procurement actions to review the J&A from the FPDS-NG data. Additionally, we requested DLA Energy and DCSO to self-identify FY2013 and FY 2014 sole source service procurements. DCSO provided a logbook and DLA Energy provided a listing of potential contract numbers. We analyzed the supplementary data provided by DCSO and DLA Energy and judgmentally selected two contracts that were not included in the FPDS-NG data and added those to our sample. This increased our total sample from six contracts to eight contracts for review.

The FPDS-NG "Not Competed" FY2013 and FY2014 data showed $93.4 million in sole service contracts. We eliminated $25.7 million in information technology contracts related to the DoDIG audit leaving 32 contracts valued at approximately $67.7 million as our universe for testing. The eight sample contracts had a value of about $16 million.

Since the sample was non-statistical the results from our review of the eight sole source service contracts cannot be projected to the universe of sole source service contracts.

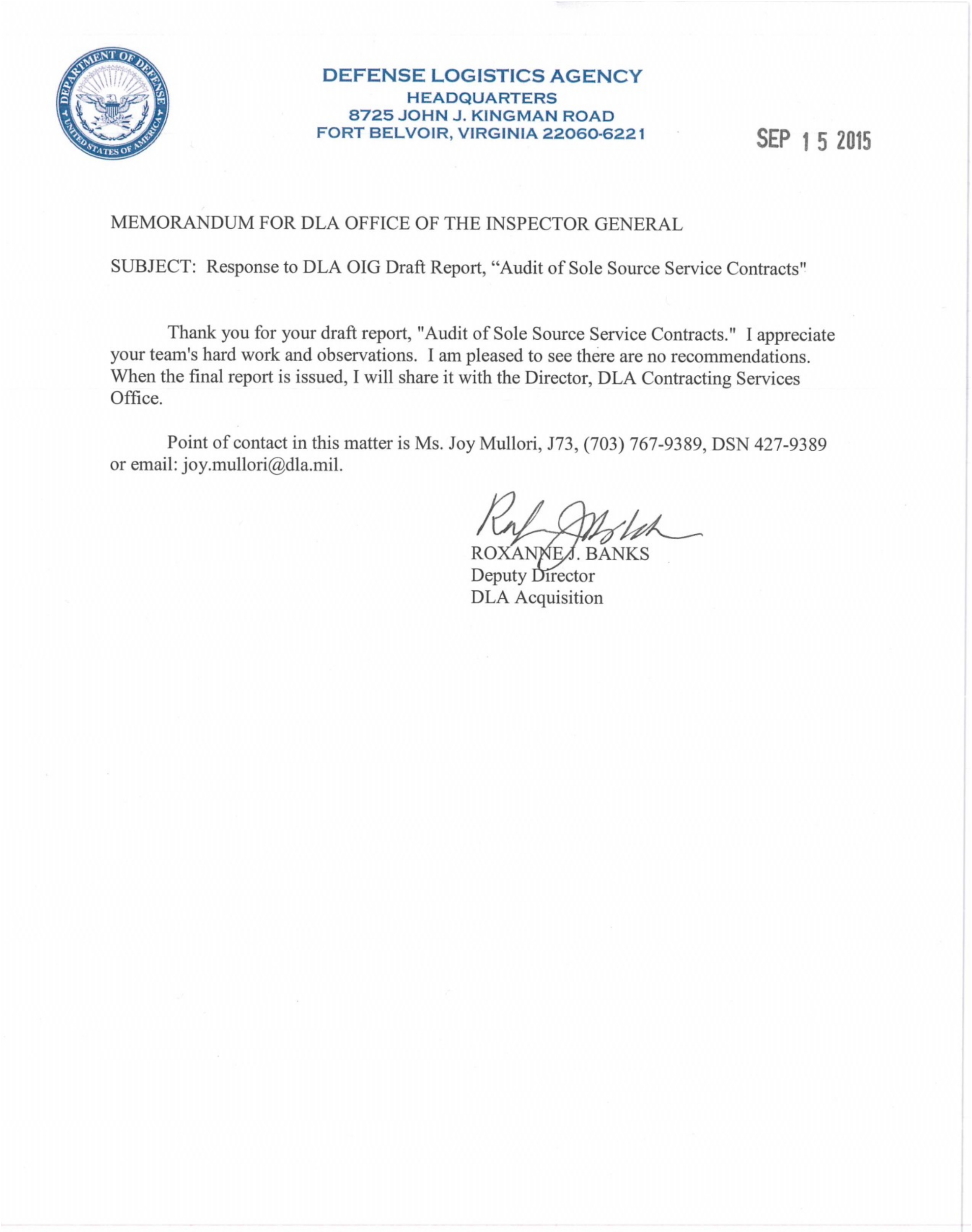
Use of Computer Processed Data

We did not rely on computer processed data for our findings, recommendations or conclusions for this report. The contract records reviewed for this audit were hard copy files.

Locations / Commands Visited

1. DLA Acquisition (J7),
2. DLA Energy, Ft. Belvoir,
3. DCSO:
    - Ft. Belvoir, VA,
    - Richmond, VA,
    - Philadelphia, PA.

APPENDIX B. MANAGEMENT COMMENTS



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

SEP 15 2015

MEMORANDUM FOR DLA OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Response to DLA OIG Draft Report, "Audit of Sole Source Service Contracts"

Thank you for your draft report, "Audit of Sole Source Service Contracts." I appreciate your team's hard work and observations. I am pleased to see there are no recommendations. When the final report is issued, I will share it with the Director, DLA Contracting Services Office.

Point of contact in this matter is Ms. Joy Mullori, J73, (703) 767-9389, DSN 427-9389 or email: joy.mullori@dla.mil.

ROXANNE J. BANKS
Deputy Director
DLA Acquisition

DLA Office of the Inspector General

DLA Implementation of the FISMA Reporting Process, DIACAP, and Selected IA Controls Audit

Audit Report: DAO-10-19 **December 27, 2011**

Executive Summary

Audit Report DAO-10-19
December 27, 2011

DLA Implementation of FISMA Reporting Process, DIACAP and Selected IA Controls Audit

Results

DLA's processes for the Federal Information Security Management Act (FISMA) reporting generally complied with the Office of Management and Budget (OMB) and DOD requirements for fiscal year 2010; however, the supporting documentation used in the FISMA report was not retained as part of the data collection process.

We also determined that DLA generally did not implement the DOD Information Assurance Certification and Accreditation Process (DIACAP) in accordance with DOD Instruction (DODI) 8510.01. We identified three control deficiencies related to DLA implementation of the DIACAP and made 10 recommendations to Management.

We concluded that 10 of 28 high-impact Information Assurance (IA) controls generally were not designed and/or operated effectively in accordance with DOD Directive 8500.01E and DODI 8500.2 for five DLA Automated Information System (AIS) applications. We identified six control deficiencies that affected multiple DLA systems (i.e., enterprise-level) and nine control deficiencies specific to the Employee Activity Guide for Labor Entry (EAGLE), Federal Logistics Information System (FLIS), Defense Medical Logistics Standard Support - Wholesale (DMLSS-W), Distribution Standard System (DSS), and Enterprise Business System (EBS).

Additionally, we determined that DLA Information Operations at Fort Belvoir had effectively eliminated 1 of 4 deficiencies reported as Notice of Deficiencies (NODs) within the Federal Information System Controls Audit Manual (FISCAM) Readiness Assessment Report, dated June 1, 2007. We also noted one observation related to the rules of behavior that merited management's attention.

The identified security deficiencies related to the DLA implementation of the DIACAP and the design and operating effectiveness of IA controls could significantly affect the security posture of DLA information systems. We noted that management is working towards identifying better solutions and business practices to help improve the security of DLA information systems.

Why DLA OIG Did this Review

The establishment and maintenance of a mature and effective IT governance framework was necessary for achieving the DLA strategic-focus area of Stewardship Excellence. In order to facilitate this evolution towards excellence, the Director of DLA approved an independent and objective assessment of the current maturity level of DLA FISMA reporting processes and the implementation of DIACAP as part of the Fiscal Year 2010 Enterprise Audit Plan.

What DLA OIG Did

Our audit objectives were to determine whether: (1) DLA's processes for FISMA reporting complied with OMB and DOD requirements; (2) DLA's implementation of the DIACAP complied with DOD Instruction 8510.01; (3) Selected IA controls were designed and operating effectively and (4) Corrective actions taken in response to NOD 8, 9, 18, and 19 related to DLA Energy systems adequately eliminated the identified deficiencies.

What DLA OIG Recommends

This report contained 50 recommendations addressed to DLA Information Operations and field sites, and DLA Troop Support. Our recommendations were intended to strengthen the internal controls surrounding DLA system security. It also contained one observation noted during testing.

DLA management either concurred or partially concurred with forty-two of our recommendations and non-concurred with eight of our recommendations.

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

December 27, 2011

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Final OIG DIACAP_FISMA Report

The DLA Office of the Inspector General (OIG) Audit Division performed this audit in response to the fiscal year 2010 Enterprise Audit Plan approved by the Director of DLA. This report discusses the results of the enterprise audit related to our four audit objectives.

Based on the audit, we concluded that DLA generally complied with fiscal year 2010 DOD and the Federal Information Security Management Act (FISMA) reporting requirements. However, DLA generally did not implement the DOD Information Assurance Certification and Accreditation Process (DIACAP) in accordance with DOD Instruction (DODI) 8510.01.

We also concluded that 10 of 28 high-impact Information Assurance (IA) controls generally were not designed and/or operated effectively in accordance with DOD Directive 8500.01E and DODI 8500.2 for five DLA Automated Information System (AIS) applications. Furthermore, we identified that the corrective actions taken did not adequately remediate all deficiencies identified as part of the four Notice of Deficiencies (NODs) as reported in the FISCAM Readiness Assessment report for DLA Energy systems.

Based on our findings, we made 50 recommendations to the Director of DLA Information Operations, Director of DLA Information Operations field sites, and Director of Medical Information Management Division at DLA Troop Support. We requested and obtained management comments on a draft of this report. Their verbatim comments are included in Appendix J. DLA management either concurred or partially concurred with forty-two of our recommendations and non-concurred with eight of our recommendations. We have addressed their comments in the final report.

We appreciate the courtesies and cooperation extended to us during the audit. For additional information about this report, contact Ms. Alice Nguyen at 703-767-6262 or by email at Alice.Nguyen@dla.mil.

Bridget A Skjoldal
for STEVEN D. PIGOTT
Assistant Deputy Inspector General
DLA OIG Audit Division

DISTRIBUTION:

DIRECTOR OF INFORMATION OPERATIONS
DIRECTOR OF INFORMATION OPERATIONS AT NEW CUMBERLAND
DIRECTOR OF INFORMATION OPERATIONS AT OGDEN
DIRECTOR OF INFORMATION OPERATIONS AT FORT BELVOIR

CONTENTS

Page

INTRODUCTION

RESULTS, RECOMMEDNATIONS, AND CONCLUSIONS

APPENDICES

INTRODUCTION

OBJECTIVES, SCOPE AND METHODOLOGY

The objectives of our audit were to determine whether:

1. DLA's processes for the Federal Information Security Management Act (FISMA) reporting comply with the Office of Management and Budget (OMB) and DOD reporting requirements.
2. DLA's implementation of the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) comply with DOD Instruction (DODI) 8510.01.
3. Selected Information Assurance (IA) controls are designed and operating effectively in accordance with DOD Directive 8500.01E and DODI 8500.2 (excluding privacy, environmental, physical security, and enclave boundary defense) for the following five DLA Automated Information System (AIS) applications:
   - Employee Activity Guide for Labor Entry (EAGLE)
   - Federal Logistics Information System (FLIS)
   - Defense Medical Logistics Standard Support – Wholesale (DMLSS-W)
   - Distribution Standard System (DSS)
   - Enterprise Business System (EBS)
4. Corrective actions taken related to Notice of Deficiencies (NODs) 8, 9, 18, and 19 issued as part of the DLA Energy Federal Information System Controls Audit Manual (FISCAM) Readiness Assessment Report, dated June 1, 2007, adequately addressed and eliminated the deficiencies.

To accomplish the above audit objectives, we selected five AIS applications, interviewed IA personnel, obtained source information from multiple sites, and selected appropriate sampling methodologies to test relevant controls. Refer to Appendix D for details of the audit scope and methodology used to complete the audit.

We conducted this audit from July 2010 to April 2011 in accordance with generally accepted government auditing standards (GAGAS) issued by the Government Accountability Office (GAO), except for organizational impairments to our independence. The organizational impairments to independence resulted from the DLA OIG not directly reporting to the head or deputy head of DLA and conducting OMB Circular A-123 non-audit services. The deficiencies resulted from an inadequate system of quality control and the lack of policies and procedures for performing and reporting audits in conformity with professional standards. We are developing corrective actions to address the organizational independence and will implement and maintain a system of quality control with the emphasis on performing high-quality work in consideration of future or ongoing performance audits. However, this has no effect on the quality of this report as GAGAS requires that we plan and conduct the performance audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusion 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.

During the audit we identified that the Defense Information Systems Agency (DISA) and the DLA Ogden Enclave (DOE) managed some controls for the selected five AIS applications, which were classified as inherited controls. We reviewed the inherited controls to ensure that DLA AIS Certification and Accreditation (C&A) package captured the information in accordance with the DIACAP requirements. We did not perform the test of design or operating effectiveness of controls that DLA AIS applications inherited from DISA and DOE. Additionally EBS ran on the SAP platform that resided on servers managed by DISA. During the audit, experts with knowledge of the EBS application and SAP platform were not available for the audit team to independently test the presence of embedded scripts containing passwords, as required by IA Control IAIA-1 (Individual Identification and Authentication).

BACKGROUND

The DLA Office of the Inspector General (OIG) solicited concerns related to potential and known risk areas from DLA Executive Board members, the DLA audit community, reviewed the GAO high-risk series, and current events. We then identified high-risk areas to DLA and incorporated them into our fiscal year 2010 Enterprise Audit Plan that was approved by the Director of DLA. Consequently, the fiscal year 2010 Enterprise Audit Plan identified the FISMA reporting process and the implementation of the DIACAP as high-risk areas.

The FISMA of 2002 was enacted to ensure Federal agencies develop a comprehensive framework to protect the government's information, operations, and assets. FISMA assigned specific responsibilities to Federal agencies, the National Institute of Standards and Technology (NIST), and the OMB in order to strengthen the security of the Federal information systems. Specifically, FISMA required the head of each agency to implement policies and procedures to reduce IT security risks to an acceptable level in a cost-effective manner. During fiscal year 2010, the Act also required quarterly and annual reporting of FISMA compliance to OMB at the department level. The Office of the Secretary of Defense (OSD) provided guidance on fiscal year 2010 reporting requirements and areas of security focus through memoranda and reporting templates. DLA used OSD issued templates to report aggregated agency-wide information captured from the DLA Information Operations field sites. The Director of DLA Information Operations signed DLA fiscal year 2010 FISMA information as the DLA Chief Information Officer, and forwarded it to OSD. DLA FISMA information was then combined with other DOD agencies and electronically submitted via CyberScope to OMB.

The DODI 8510.01 was the DOD implementation of the policies and procedures to reduce IT security risks to an acceptable level and established a C&A process to manage the IA capabilities and services. DLA established the DLA DIACAP Implementation Guide, version 1.2, dated March 2009 to provide clarification on DLA specific C&A and security requirements for DLA information systems.

As part of the C&A process, the minimum IA controls were based on the Mission Assurance Category (MAC) and the Confidentiality Level of the information system detailed in DODI 8500.2. Through the DLA Implementation Guide, the Director of DLA Information Operations made the decision to facilitate the execution of the DIACAP through the use of the automated system provided by the DLA instance of the Enterprise Mission Assurance Support System (eMASS). eMASS was a Government owned, non-proprietary, set of integrated Web services, which provided visibility and automation of IA program management processes. All C&A submissions (reaccreditation and annual IA control validation) for DLA information systems must be completed using eMASS.

Furthermore, the accounting firm KPMG LLP identified four NODs related to IA controls during their 2007 FISCAM Readiness Assessment of DLA Energy financial systems. DLA Information Operations at Fort Belvoir addressed the required actions associated with each NOD as corrective actions to remediate the identified IT deficiencies. Refer to Table 1 below for the required actions KPMG issued as part of the NOD 8, 9, 18, and 19.

Table 1. Description of DLA Energy NODs and Required Actions

NOD #	Description	Summary of Required Actions
8	C&A of the Requirements Manager (RM) Application	1. Certify and accredit RM application and general support system in accordance with DLA, DOD, NIST, and OMB Guidance.
9	Centralized management of plan of action and milestones (POA&M)	1. Centralize a process to ensure that all IT security weaknesses identified during any internal or external reviews done by, for, or on behalf of the agency, are included in a centralized POA&M report.
		2. Update POA&M policies and procedures to include steps on how to close out a POA&M issue, updating the status of open findings, and assigning a point of contact, for addressing the finding.
		3. Ensure that each office is aware of each others' effort to resolve and/or mitigate outstanding POA&M IT security issues.
18	Access and security control information within the certification and accreditation package	1. Update the BSM-E and DFAMS, PORTS security documents in support of the C&A process to include: (a) An overview of the security controls provided by the system software used to support the application (operating system and database) (b) Details on the security controls that each application's system software provides to the application it supports (e.g., available access functions, description of the functions, and combination of functions that users can and cannot have.) (c) Application and system software documentation regarding segregation of duties, as well as formally defining all available roles for more effective management tracking and oversight of sensitive functions.
19	Continuity of operations planning, training, and testing	1. Update the DFAMS and DISA DECC Ogden Contingency Plans. Ensure to include the current data center environment controls and training requirements.
		2. Update the BSM-E Contingency Plan to include the RM Application.
		3. Perform a BSM-E COOP Test exercise, include the applications and system that the exercise covers.
		4. Update the DFAMS contingency plan to include procedures and documentation requirements over the restoration and testing of backup tapes.

Source: DLA OIG Developed

DLA Energy had been through a system modernization project, called Energy Convergence (E-Convergence). E-Convergence may replace some DLA Energy systems, such as Business Systems Modernization-Energy (BSM-E), and Defense Fuels Automated Management System (DFAMS). DLA Information Operations and DLA Energy had decided against continuing remediation efforts on any NODs related to system documentation, system access controls and general controls. Corrective actions for the NODs would be included into the system requirements for E-Convergence and DLA's coordination with the DOD Office of Inspector General (DOD IG), and DISA IG to include general controls as part of the DISA Statement of Auditing Standards 70 audit.

RESULTS, RECOMMENDATIONS, AND CONCLUSIONS

RESULTS AND RECOMMENDATIONS

In this section, we addressed the results from our four main audit objectives and the related findings and recommendations.

I. FISMA REPORTING PROCESS

The intent of FISMA was to strengthen the safeguarding of information systems operated by the United States government. Each executive department was required to evaluate their agency's information security programs and report the results to OMB, Congress, and GAO in November of each year. The OSD's fiscal year 2010 FISMA reporting template required DLA to report information in the area of system inventory; asset management; configuration management; vulnerability management; identity and access management; data and boundary protection; training and education; and remote access/telework.

Data Retention for FISMA Reporting

DLA met the OMB and DOD FISMA reporting requirements for fiscal year 2010; however, DLA Information Operations did not retain supporting documentation for the data reported within the DLA FISMA reporting template. This occurred because DLA had not formalized a FISMA reporting process to require the retention of FISMA reporting data. Therefore, DLA FISMA compliance information reported to OSD could not be confirmed.

The GAO Standards for Internal Control in the Federal Government, dated November 1999, stated, "All transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation…may be in paper or electronic form. All documentation and records should be properly managed and maintained."

DLA Information Assurance groups at various sites scanned site network segments using the Host Based Security System and Retina utilities, in order to gather all required system and device information for 2010 FISMA reporting. DLA also utilized the Learning Management System and Skillsoft to obtain civilians, active duty military, contractors, and reservists' annual IA awareness training information in order to complete the training & education area of the FISMA reporting template. All these tools tracked and reported IT assets connected to the network and user's IA awareness training progress at a specific point in time. Additionally, the DLA Information Operations and field sites also made adjustments to the IT assets or IA awareness training data generated from the automated tools as part of the data aggregation process to correct any errors identified before reporting the FISMA compliance information to OSD.

Although DLA Information Operations had implemented controls to gather the necessary FISMA compliance information and reported it to OSD, they did not retain the reports generated and supporting documents for adjustments made during the data collection process. Therefore, the information reported within the fiscal year 2010 FISMA reporting template to OSD could not be validated in order to determine the accuracy of data that the DLA Information Operations used to arrive at the correct FISMA compliance results.

This occurred because DLA relied on DOD guidance and reporting templates to gather the necessary data to demonstrate compliance with FISMA requirements. Also, the security areas required for FISMA reporting had changed each reporting period. Since OSD was consistently late in its delivery of guidance to DOD components, DLA had not formalized a FISMA reporting process to include establishing a formal policy and procedure requiring the retention of FISMA reporting data. As a result, DLA Information Operations could not readily provide evidence to support the reasonableness or accuracy of DLA FISMA compliance information that was submitted to the OSD.

Recommendation 1 *(Director, DLA Information Operations)*

Develop policy and procedure for retention of supporting data used for FISMA reporting.

Management Comments

Partially Concurred. DLA HQ IT Continuity of Operations Plan (COOP) Team developed a collaboration room for retention of supporting data used for FISMA reporting. This collaboration site is a joint repository for J6 FISMA report data. Verbatim management comments can be found in Appendix J

DLA OIG Response

Management comments were nonresponsive. Management's comments did not address the development of a policy and procedure that set the requirement for retention of supporting data used for FISMA reporting.

II. DLA IMPLEMENTATION OF THE DIACAP

DLA facilitated and executed DIACAP through the use of the automated capabilities of eMASS. DLA required all C&A submissions (i.e., reaccreditation and annual IA control validation) for DLA information systems be conducted using eMASS. The tool facilitated the responsible personnel to enter information system data, track the progress of the C&A activities (e.g., IA control implementation and validation, etc.), and track associated Plan of Action and Milestones (POA&M) status for the purpose of conveying system security information and compliance status.

We identified three deficiencies related to the DLA C&A process for EAGLE, FLIS, DMLSS-W, DSS, and EBS. See Table 2 below for a summary of the deficiencies and the affected AIS applications.

Table 2. DLA Certification & Accreditation Process Deficiencies

Areas of Deficiencies	Systems Selected				
	EAGLE	FLIS	DMLSS-W	DSS	EBS
Validation of Test Results and Supporting Artifacts	✗	✗	✓	✗	✗
Service Level Agreements	✗	✗	N/A	✗	✗
POA&M Management	✗	✗	✗	✗	✗

Legend	
✓	No deficiency identified related to the selected system.
✗	Deficiencies identified for selected system.
N/A	DMLSS-W did not have a direct service level agreement with DISA.

Source: DLA OIG Developed

Validation of Test Results and Supporting Artifacts

DLA Information Operations, Information Assurance, performed IA certification reviews to verify the proper assignment, implementation, and compliance status of all applicable IA controls before certification determination; however, there was no guidance on the types of required documentation to support security validation results that needed to be a part of the system C&A package. Consequently, DLA systems could have received an authorization to operate with severe security risks that could have compromised the confidentiality, integrity, and availability of DLA information systems.

The DLA DIACAP Implementation Guide required the assignment of baseline IA controls, to include identification of IA controls inherited from other information systems. The Guide required the DLA CA's certification determination be based in part on the System CA Representative's recommendation, actual validation results, and additional processes and procedures undertaken by the DLA Information Operations – Information Assurance office. Also, the Guide required the program or system manager to obtain validation test results and applicable supporting artifacts for inherited IA controls. Further, DODI 8510.01 required a program or system manager be identified for each DOD Component information system.

Based on a review of EAGLE, FLIS, DSS, and EBS C&A packages, we identified the following deficiencies with the information reported in the packages:

- Validation test results and applicable supporting artifacts for inherited IA controls were not available for EBS, DSS, FLIS, and EAGLE.
- Some inherited controls and shared controls were improperly assigned in the DLA system DIACAP packages. For example,
    - EBS account management control [1] was assigned as an inherited control when it should have been assigned as a shared control;
    - FLIS assigned the virus protection control [2] as an inherited control when it should have been assigned as a control that was not applicable; and
    - EAGLE assigned the system state changes [3] and security configuration compliance[4] IA controls as DLA-owned controls when they should have been assigned as inherited controls.
- DSS received an authorization to operate with a CA Representative, who also acted as the designated Program or System Manager, which was not an allowable relationship among DIACAP team members as outlined in DODI 8510.01.

Based on the current DLA C&A process, the DLA Information Operations, Information Assurance, C&A Package Verification Team only verified information that was uploaded into eMASS. Additionally, DLA Information Operations IA Compliance Review Team only validated IA controls for DLA enclaves. The improper assignment of inherited IA controls and the deficiency of not having validation test results and compliance status for inherited IA controls were due to a lack of management oversight, as well as eMASS system limitations on the assignment of shared controls. Additionally, DLA Information Operations at New Cumberland did not assign a program or system manager to DSS due to a lack of management oversight.

Without proper IA control validation procedures, the DLA CA could not ensure that IA controls were sufficiently designed and operating effectively, in order to make an informative certification determination and accreditation recommendation to the DLA DAA; which was the basis for a final authorization to operate decision. Improper assignment of IA controls might lead DLA to place reliance on security controls from originating systems (i.e., DISA) that did not exist; therefore, exposing DLA information systems to security risks that could negatively affect DLA's ability to accomplish the mission.

[1] IA control number for account management control was IAAC-1.

[2] IA control number for virus protection control was ECVP-1.

[3] IA control number for the system state changes was DCSS-1.

[4] IA control number for the security configuration compliance was ECSC-1.

In addition, without a designated program or system manager, DSS may not have a dedicated individual for the execution of the DIACAP to ensure that information system security engineering was employed to implement or modify the IA component of the system architecture.

Recommendation 2 *(Director, DLA Information Operations)*

Update and enforce the validation process in order to assess and document the design/operating effectiveness of all IA controls for DLA systems.

Management Comments

Non-Concurred. The validation process was clearly defined in Department of Defense (DOD) Instruction (DODI) 8510.01 and the DLA DIACAP Implementation Guide, plus the DIACAP Knowledge Service Web Portal went into specific detail with regards to the assessment steps, required artifacts, expect results, etc. for every IA control to be assessed. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. Even though the validation procedures were maintained through the DIACAP Configuration Control and Management and published in the DIACAP Knowledge Service Web Portal, they did not seem to be sufficient to identify deficiencies in the design and operating effectiveness of IA controls. We identified multiple misclassifications of IA controls within the EBS, FLIS and EAGLE C&A packages, missing validation results for inherited controls, and inadequate validation activities that did not detect high risk control deficiencies, such as EAGLE's application developers having access to production.

Recommendation 3 *(Director, DLA Information Operations)*

Re-evaluate all applicable IA controls and confirm the correct assignment of inherited, shared, and DLA-owned baseline IA controls for each DLA system in eMASS.

Management Comments

Partially Concurred. DLA Information Operations determined that an evaluation of all applicable IA controls was already part of the DLA DIACAP implementation. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. The IA controls were inaccurately assigned in eMASS within the EBS, FLIS, and EAGLE C&A process. Also, eMASS did not have the capability to accurately reflect whether IA controls were inherited, shared, and DLA-owned IA controls during our audit. We adjusted our original recommendation to clarify the remediation actions in order to improve DLA security posture.

Recommendation 4 *(Director, DLA Information Operations)*

Enforce the requirement that a program or system manager be designated for each DLA system and who will perform the functions in accordance with DODI 8510.01 and the DLA DIACAP Implementation Guide.

Management Comments

Partially Concurred. Designation of either SM or PM is a requirement per DODI 8510.01 and the DLA DIACAP Implementation Guide. However, no DLA DIACAP package has been approved without a SM/PM assigned in eMASS and it is the incumbent on the system owner (e.g., J6 Field Site Director) to ensure that the assignment of a responsible SM/PM is done in a manner in which the individual assigned is responsible for all the inherent responsibilities of such an assignment. DLA has updated DLA Instruction 6401, "IA Management Controls" to reinforce this requirement. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive. DSS did assign a designated PM. However, the DSS SM/PM and the CA Representative was the same individual, which was not an allowable relationship among DIACAP team members as outlined in DODI 8510.01, because the CA Representative role within DLA was an extension of the CA role.

Service Level Agreements

The current Director of DLA or one of the expressed designees did not sign the Enterprise Service Support Document (ESSD) and Service Level Agreements (SLAs) with DISA, which was needed to create a valid contract between the two organizations, as required by the Delegations of Authority Memorandum, issued on February 17, 2011. Also, the current DLA ESSD and SLAs neither outlined the application-specific listings of the inherited, shared, and customer-owned IA controls nor clearly defined the IA roles and responsibility between DLA and DISA for the EAGLE application. The deficiencies with the current DLA ESSD and SLAs may increase security risks for DLA information systems. Consequently, DLA could not perform comprehensive risk assessments and implement the correct security measures to protect DLA systems.

The Delegations of Authority Memorandum, dated February 17, 2011, from the Director of DLA, stated "within 60 days from the date of this memorandum, each Primary Level Field Activity (PLFA), Staff Directorate, and all other organization entities within DLA shall conduct a comprehensive review of all existing agreements with non-DLA entities such as a Combatant Command, a Military Service, another DOD Agency, non-DLA Agencies including State and Local Governments, or a foreign government." Additionally, the memorandum stated, "requests for such delegations of authority to act on behalf of DLA must be submitted in writing through the Director, DLA Logistics Operations, and must include the specific delegation requested…." Furthermore, DODI 8500.2 required that the Government, service provider, and end user IA roles and responsibilities be explicitly addressed for IT services acquisition or outsourcing of IT services.

Based on a review of the current DLA ESSD and SLAs between DLA and DISA, we identified the following deficiencies:

- FLIS, DSS, and EBS recently downgraded from MAC level II to level III in September 2010; however, the SLAs for these systems were not resigned to formalize the changes in the level of services provided.

- The SLAs for FLIS, DSS, and EBS did not contain application-specific listings of the inherited, shared, and customer-owned IA controls.

- EAGLE was fully deployed and hosted by DISA in 2009. However, the DLA ESSD was not updated to include EAGLE as one of the DLA systems being hosted at DISA.

- The SLA for EAGLE did not clearly identify IA roles and responsibilities between DLA Information Operations at Ogden and DISA.

- EAGLE personnel reviewed the planning estimates, which contained financial information from the services furnished by DISA as defined within the SLA; however, there was no evidence of an annual review of the SLA for EAGLE.

This occurred because the length of time to establish a formal agreement between DLA and DISA was typically very long due to multi-level reviews. Additionally, DLA and DISA utilized a standard SLA template; therefore, a system-specific listing of inherited, shared, and customer-owned IA controls for DLA systems was not included as part of the formally signed SLAs. Formal changes to the information within the ESSD and SLAs occurred at DLA Information Operations; however, DLA Information Operations at Ogden did not receive guidance on specific items within the EAGLE SLA that needed to be reviewed for possible revision on an annual basis.

Without a valid contractual agreement between DLA and DISA, DLA management could not hold DISA accountable to perform the IA roles and responsibility defined within the terms and conditions of the agreement. Without a system-specific listing of inherited, shared, and customer-owned IA control listing, DLA IA personnel may incorrectly place reliance on critical IA controls that were not provided by DISA. As the result, comprehensive risk assessments of DLA systems could not be adequately performed to provide the DLA DAA with the correct information for the final authorization to operate decision. Additionally, DLA may reimburse DISA for the incorrect level of support, which could prevent funding for other key programs and activities in support of the DLA mission.

Recommendation 5 *(Director, DLA Information Operations)*

Coordinate with the Director of DLA or obtain the delegation of authority to update the DLA ESSD and SLAs with DISA, to explicitly define the expected level of services, and IA roles and responsibilities.

Management Comments

Concurred. This recommendation requires DISA to update its internal SLA document template. DLA has no authority to compel DISA to change their ESSD document template as it is another DOD Agency. DLA Enterprise Solution and DISA have established a team reviewing the DLA ESSD to ensure an enterprise approach is implemented, clear IA boundaries are identified, and the service levels are clearly defined. The estimated completion date to implement this recommendation is December 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 6 *(Director, DLA Information Operations)*

Coordinate with DISA to explicitly define listings of system-specific inherited, shared, and customer-owned IA controls for all DLA systems hosted by DISA.

Management Comments

Concurred. This recommendation requires DISA to update its internal SLA document template. DLA has no authority to compel DISA to change their ESSD document template as it is another

DOD Agency. DLA Enterprise Solution and DISA have established a team reviewing the DLA ESSD to ensure an enterprise approach is implemented, clear IA boundaries are identified, and the service levels are clearly defined. The estimated completion date to implement this recommendation is December 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 7 *(Director, DLA Information Operations)*

Communicate guidance to the Director of DLA Information Operations at Ogden on the minimum information that must be reviewed and communicated back to DLA Information Operations update the SLAs with DISA on an annual basis.

Management Comments

Concurred. DLA and DISA had established a team to work with all DLA stakeholders to ensure communication is clear. SLAs are part of the ESSD revision and DLA Information Operations at Ogden are included as stakeholders. The estimated completion date to implement this recommendation is December 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Plan of Action and Milestones (POA&M) Management

The execution, tracking, managing, and closure process related to IT POA&Ms were not operating effectively. DLA Information Operations did not establish a standard procedure to enforce requirements for the IT POA&M preparation, monitoring, and closure. Without a comprehensive POA&M process, IA control weaknesses may not be addressed in a timely manner to protect the confidentiality, integrity, and availability of DLA systems.

DODI 8510.01 required each DOD Component to use one of the following terms to report status of corrective actions: ongoing, completed, or risk accepted for a Category (CAT) II or CAT III weakness. The term "Completed" should be used only when a security weakness had been fully resolved and the corrective action had been tested. The Instruction also required the DAAs be responsible for monitoring and tracking overall execution of system-level IT POA&Ms.

In addition, the DLA DIACAP Implementation Guide required that a POA&M be a permanent record that identified tasks to be accomplished in order to resolve security weaknesses. A POA&M was required for any accreditation decision that required corrective actions and it specified resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks. It was also used to document non-compliant IA controls accepted by the DAA and baseline IA controls that were not applicable. Furthermore, the DLA DIACAP Implementation Guide required the program or system manager to obtain validation test results and applicable supporting artifacts for inherited controls. The DLA DIACAP Implementation Guide also required DLA information systems with a current authorization to operate that were found to be operating in an unacceptable IA posture through GAO audits, DOD IG audits, etc., to have the newly identified weakness/vulnerability added to an existing or newly created POA&M.

We identified the following deficiencies related to the execution, tracking, managing, and closure of IT POA&Ms:

- Residual risk analyses were not consistently documented for IT weaknesses identified in the POA&Ms for EAGLE, FLIS, DMLSS-W, DSS, and EBS, as part of the DIACAP. Additionally, mitigating controls implemented to reduce existing security risks were not documented as part of a residual risk analysis. For example, EAGLE contained edit checks to prevent time and attendance information from being submitted for terminated users; and EAGLE, FLIS, DSS, and EBS, had an automatic feature to disable user accounts after 30 days of inactivity.

- The IT weaknesses identified internally from the DLA OIG audit reports and externally from the DOD IG audit reports for EBS and DSS were not tracked and managed as POA&Ms in eMASS.

- Some EBS POA&Ms were marked “Completed” before the actual implementation of the resolution. For example, a POA&M on the DLA Internet Bid Board System/Supplier Requirements Visibility Application (DIBBS/SRVA) was marked “Completed” without evidence of a remediation plan for the identified risks, or evidence that security weaknesses had been fully resolved and the corrective action had been tested.

- EAGLE, FLIS, DSS, and EBS Information Assurance Managers (IAMs) did not have visibility into weaknesses related to the design and operating effectiveness of the IA controls inherited from DISA.

- The current POA&M management process implemented by DLA Information Operations did not completely address the weaknesses identified in the DLA Energy FISCAM Readiness Assessment NOD 9. Specifically, DLA Information Operations did not have a comprehensive process to ensure that all IT security weaknesses identified during any internal or external reviews were included in POA&Ms and a verification procedure for POA&M closure that were recommended as part of NOD 9 required actions.

The DLA DIACAP Implementation Guide and DOD Instructions did not have specific guidance on the information needed to be documented as part of the residual risk analyses for each IT weakness. IT findings identified as part of DLA internal or external reviews (i.e., GAO audits, DOD IG, DLA OIG audits, etc.) were not consistently disseminated to IA personnel responsible for the affected DLA systems, to create POA&Ms, and to track corrective actions to completion. Additionally, due to a lack of management oversight, POA&Ms were marked as "Completed" without evidence that the security weaknesses had been fully resolved and the corrective actions had been tested.

Additionally, due to the complicated information requesting process, DLA personnel had difficulties obtaining compliance status and POA&Ms information related to inherited controls for DLA systems hosted at DISA. DISA did not utilize eMASS to capture the compliance status of its IA controls and POA&Ms for its systems; therefore, DLA could not automatically link inherited control weaknesses from DISA to DLA systems through eMASS.

In order to provide the DAA with a comprehensive status of the IA posture for a system, security weaknesses associated with IA controls inherited from another system under a separate accreditation boundary (i.e., DISA) needed to be reflected on the receiving system IT POA&Ms. With POA&Ms information missing, the DAA would not have complete and accurate information on the security posture of the system to make an informed authorization to operate decision.

Recommendation 8 *(Director, DLA Information Operations)*

Update the DLA DIACAP Implementation Guide to provide detailed instructions on the standard format and appropriate artifacts to support the residual risk analysis for IT security weaknesses reported on the POA&Ms.

Management Comments

Non-Concurred. The DLA DIACAP Implementation Guide clearly establishes the requirement for documenting all identified IA control related system weaknesses. Additionally, the "Preparation of IT security POA&Ms" policy memorandum signed by the J6 Director in March 2009 documented requirements and guidance for POA&M requirements. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. The DLA DIACAP Implementation Guide and the Preparation of IT Security POA&M established the requirement for documenting all identified IA controls related system weaknesses. However, those requirements did not include instructions on the documentation of residual risk.

Recommendation 9 *(Director, DLA Information Operations)*

Implement an enterprise procedure for disseminating, tracking, and managing DLA IT security weaknesses identified as the results of internal or external assessments or audits (i.e., IA security assessments during the C&A process, annual system security review, GAO audit, DOD IG audits, and DLA OIG audits).

Management Comments

Non-Concurred. DLA DIACAP implementation is the procedure for disseminating, tracking, and managing DLA IT security weaknesses identified as the result of internal or external assessments or audits. This is also supplemented by "Preparation of IT Security POA&Ms" policy memorandum which notes the distinction of whether or not all weaknesses identified during internal or external audits should be documented in the IT Security POA&M. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. External and internal IT weaknesses identified from other audits were not being captured as POA&Ms for the AIS applications selected for an audit; therefore, DLA Information Operations field sites were not in compliance with the requirements for tracking IT security weaknesses as part of the DLA DIACAP Implementation Guide and the "Preparation of IT Security POA&Ms" policy memorandum.

Recommendation 10 *(Director, DLA Information Operations)*

Develop and implement a process for validating evidence that corrective actions for security weaknesses have been fully resolved and the corrective actions have been tested for the deficiencies before marking POA&Ms "Completed."

Management Comments

Non-Concurred. DLA Information Operations, Information Assurance has established a POA&M Tracking Program, in which every POA&M item for all accredited information systems are tracked via a monthly meeting to discuss the current status, to include milestone completion date changes and mitigation/corrective action implementation progress. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. Even though DLA Information Operations, Information Assurance conducts a monthly meeting to discuss the current status of POA&M items, the POA&M Tracking Program does not include an independent testing of the corrective actions to ensure that they are sufficient to resolve the control weaknesses prior to categorizing a POA&M as “Completed” in eMASS.

Recommendation 11 *(Director, DLA Information Operations)*

Coordinate with DISA to obtain validation test results and applicable supporting artifacts for inherited IA controls.

Management Comments

Concurred. DLA Information Operation, Information Assurance has reached an agreement with DISA Computing Services Division (CSD) on the transparency of Information Assurance (IA) control reviews performed in the validation of inherited IA Controls. The estimated completion date to implement this recommendation is November 2011. This agreement dealt with the 32 IA controls identified in the DISA CSD Catalogue of Services. However, the documented evidence supporting the compliance statue of the 32 IAA controls inherited by default from DISA CSD still needs to be obtained. Furthermore, the IA controls beyond the 32 IA controls identified in the DISA CSD Catalogue of Services, are the responsibility of the inheriting information system owner (e.g., J6 Site Director, PEO, SM/PM). Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

III. INFORMATION ASSURANCE CONTROLS

We found that 18 of 28 baselined high-impact IA controls for EAGLE, FLIS, DMLSS-W, DSS, and EBS, were designed and operating effectively as intended to protect DLA AIS applications. However, improvements were needed for 10 high-impact IA controls.

Of the 10 high-impact IA controls that needed additional improvements, six were categorized as enterprise-level findings and four were categorized as system-specific findings. Enterprise-level findings were IA control areas that affected multiple DLA systems and system-specific findings were IA control areas that were isolated to the selected systems. The details of system-specific findings and recommendations could be found in Appendix E through I.

We identified six enterprise-level findings within the subject areas of continuity, security design and configuration, identification and authentication, and personnel. Refer to Table 3 below for a summary of the enterprise-level findings.

Table 3. Enterprise-Level Findings Summary

Area of Deficiencies	IA Control Number	Control Name	Subject Area	IA Service	System Selected				
					EAGLE	FLIS	DMLSS-W	DSS	EBS
Alternate System Recovery Site	COBR-1	Protection of Backup and Restoration Assets	Continuity	Availability	✗	✓	✗	✓	✗
	COTR-1	Trusted Recovery	Continuity	Availability	✗	✓	✗	✓	✗
System Security Documentation	DCSD-1	IA Documentation	Security Design and Configuration	Availability	✗	✗	✗	✗	✗
User Account Management	IAAC-1	Account Control	Identification and Authentication	Confidentiality	✗	✗	✗	✗	✗
DLA Personnel Security	PRAS-1	Access to Information	Personnel	Confidentiality	✗	✗	✗	N/A	✗
DLA Information Assurance Awareness Training	PRTN-1	Information Assurance Training	Personnel	Integrity	✗	✗	✗	✗	✗
External DLA System Users	PRAS-1	Access to Information	Personnel	Confidentiality	✗	✗	✗	✗	✗
	PRTN-1	Information Assurance Training	Personnel	Integrity	✗	✗	✗	✗	✗

Legend

✓	IA control deficiency was not identified for the selected system.
✗	IA control deficiency was identified for the selected system.
N/A	Personnel Security could not be tested for DSS Eastern region because a system generated list of DSS user could not be provided.

Source: DLA OIG Developed

Alternate System Recovery Site

The EAGLE and DMLSS-W applications did not have designated alternate system recovery sites. Additionally, during testing the following deficiencies were observed regarding EBS Continuity of Operations Planning (COOP):

- Alternate recovery site documentation in eMASS used to store the C&A package inaccurately stated that an alternate site was not designated.
- EBS database restoration was conducted as part of COOP testing at the DISA facility in Mechanicsburg, PA but was not communicated to the application Information Assurance Manager;
- COOP documentation was not available;

- The EBS recovery testing documentation listed EBS as a MAC level II system when it was a MAC III level system; and
- The July 2010 after actions report and the service request form submitted to DISA indicated that the existing backup and recovery infrastructure at the DISA facility in Mechanicsburg, PA would not be able to sustain production and recovery requirements in the future due to the aging hardware.

DODI 8510.01detailed the process for achieving and maintaining the proper IA posture through adherence to specific IA controls that were based on the information system type, the MAC, and the Confidentiality Level. DODI 8500.2 required that an alternate site be identified that had the capability to at least partially restore mission or business essential functions for MAC III systems. Therefore, as part of the DIACAP, DOD systems should comply with IA controls related to the development and testing of COOP and alternate recovery site designation.

For business availability and continuity planning purposes, agencies designated alternate system recovery sites for IT systems that support mission or business essential functions. A catastrophic failure was defined as a sudden and total failure of the system where it suffered from structural damage and immediate recovery was impossible. An alternate recovery site would permit the restoration of all mission or business essential functions after a catastrophic failure. Furthermore, management had not changed the current recovery strategy for EBS at DISA Mechanicsburg, PA facility even though reliance on restoration of data tapes alone to recover key EBS databases had been documented as an area of concern.

EAGLE and EBS were classified at MAC III, with recovery time objectives of 3 day, and 10-14 days respectively. However, since viable alternate recovery sites were not in place for EAGLE and DMLSS-W, and the designated recovery site for EBS may not be viable; hardware, software, and technical expertise may not be available or be identified to resume operation of the systems within the required recovery timeframe. In addition, COOP plans could not be accurately developed, updated, or tested to reflect the necessary actions at the alternate system recovery sites. As a result:

- The unavailability of DMLSS-W would hinder the delivery of life-saving medical products to the war fighters.
- The unavailability of EAGLE would increase the risk of inaccurate or incomplete employee time and attendance reporting and improper payroll payments.
- The unavailability of EBS would delay DLA from issuing procurements to vendors for materials, equipment, and services in support of the war fighters. Additionally, DLA would not be able to collect funds from customers and make payments to vendors to continue functioning as a working capital fund entity. Subsequently, financial information would not be accurately captured or reported to meet compliance with federal laws and regulations.

Recommendation 12 *(Director, DLA Information Operations)*

Designate viable alternate system recovery site(s) for EAGLE and DMLSS-W, update COOP documentation, and perform COOP testing. In the interim:

1. Create a POA&M in order to establish and implement mitigating controls until designated alternate system recovery site(s) are established, such as selecting temporary system recovery site(s);
2. Provide an estimated timeline to have designated alternate system recovery site(s) in place and operational; and
3. Update COOP documentation for each system to reflect the designated alternate system recovery site(s), the correct MAC level, and perform COOP testing using the recovery site(s).

Management Comments

Concur. DLA Information Operations stated the following:

- IT sites were instructed to create a Business Impact Analysis (BIA) for the EAGLE and DMLSS-W applications and to present the completed BIAs to the Director of DLA Information Operations. Additionally, each IT site was instructed to create POA&Ms that mitigate ineffective contingency controls until the designated alternate recovery location is operational and complies with established Memorandum of Agreements (MOA) with the other DLA sites.
- The estimated completion date to have a designated alternate recovery site in place for the DLA Ogden Enclave that included the EAGLE and DMLSS-W systems was March 31, 2012. Additionally, The DLA HQ IT COOP Team would coordinate with IT Program Managers the update of BIAs to reflect current system MAC levels and to schedule functional exercises at the alternate recovery site after March 31, 2012.

Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 13 *(Director, DLA Information Operations)*

Implement activities to improve the viability of EBS alternate system recovery site. For example,

- Update the C&A documentation in eMASS to accurately reflect the designation of the DISA, Mechanicsburg, PA facility as the alternate recovery site;

- Complete the coordination with the key stakeholders and user representatives to develop a Business Impact Analysis document and to create and/or update a business continuity-planning document and the IT continuity plan; and
- Ensure the completion of an upgrade to the backup and recovery infrastructure at DISA facility in Mechanicsburg, PA in order to meet future requirements.

Management Comments

Partially Concurred. DLA Information Operations, Information Assurance and Enterprise Solutions would work with the Information Assurance Officer (IAO) to make the necessary corrections in eMASS regarding the COAS-1 controls for EBS since EBS does have an alternate recovery site. Also, EBS IT COOP was updated to include business continuity planning (as of April 4, 2011) and all necessary signatures (as of September 8, 2011). However, DLA did not own the building in Mechanicsburg, PA, as it was a DISA facility; therefore, the upgrade to the infrastructure is DISA's responsibility. DLA Information Operations planned to enhance the Enterprise Telecommunications Network (ETN) to permit recovery. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive. However, DLA Information Operations should assess the feasibility of the infrastructure at the DISA facility and request DISA to correct any deficiencies if needed, in order to ensure a robust and effective recovery strategy for DLA's core accounting system.

<u>System Security Documentation</u>

All five selected DLA AIS applications were not consistent in meeting the requirements of having a System Security Plan (SSP). DLA Information Operations had not provided clear guidance on the system security documentation requirements for system certification in eMASS; therefore, DLA IA personnel for each system interpreted the OMB Circular A-130 SSP requirements based on industry best practices and past experiences. As the result, DLA Information Operations management would not be able to assess the adequacy of the controls to protect DLA critical information system resources.

OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," required the establishment of an application security plan that included security controls for all general support systems and major applications. The security plans should have addressed application rules, specialized training, personnel security, contingency planning, technical controls, information sharing, and public access controls. In addition, DODI 8500.2 required that an SSP describe the technical, administrative, and procedural IA program and policies that governed the DOD information system, and identification of all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup or emergency response). NIST Special Publication 800-18 required that the SSP provide an overview of the security requirements of the system and described the controls in place for meeting those requirements. The SSP also should delineate responsibilities and expected behavior of all individuals who access the system and it should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.

Upon a review of EAGLE, FLIS, DMLSS-W, DSS, and EBS supporting documentation we identified the following inconsistencies:

- The EAGLE, FLIS, and DMLSS-W had system-level artifacts that resembled SSPs in eMASS; while DSS and EBS utilized the information and the IA control-specific artifacts within eMASS as their SSPs.
- Some of the information contained within the system level artifacts that resembled SSPs did not match the information within eMASS. For example, inconsistent information documented on the IA personnel between the system–level artifact SSPs and information within eMASS for EAGLE, FLIS, and DMLSS-W.
- Some of the IA specific artifacts for DSS and EBS did not have the minimum security controls documentation stored within eMASS to completely address the SSP requirements. For example, the access control policy for EBS was not stored within eMASS.

The DLA DIACAP Implementation Guide and the eMASS Implementation Guide did not provide clear requirements regarding supporting documentation for certification (i.e., residual risk statement(s), actual validation results, and artifacts associated with the implementation of assigned IA controls). Specifically, the Guide did not provide a mandatory listing of required system-level artifacts, IA control-specific artifacts, or standard templates for the required artifacts. Without consistent information for system security plans in eMASS, the DLA DAA would not have a complete picture of the security posture of the system to grant an authorization to operate.

Recommendation 14 *(Director, DLA Information Operations)*

Establish, at a minimum, a list of supporting documentation or artifacts that are required as part of the DLA system certification process (i.e., system-level or IA control-specific artifact) to meet OMB Circular A-130 requirement for a SSP.

Management Comments

Non-Concurred. The DODI 8510.01 is the DOD's guidance for adherence to the requirement documented in the Office of Management and Budget (OMB) Circular A-130, Appendix III. The resulting DIACAP Scorecard contains the same information as the DIACAP Technical Advisory

Group prescribed SSP; therefore, alleviates the requirement for the development of a separate and distinct SSP. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. Since DLA management had not defined the minimum artifacts that must be available in eMASS as part of the C&A package, we noted inconsistent documentation for the same IA controls contained in eMASS for the audited AIS applications. Management should establish a minimum list of required artifacts to be maintained in eMASS that would address OMB circular A-130 requirements for a SSP.

Recommendation 15 *(Director, DLA Information Operations)*

Standardize the required artifacts in support of the C&A process, such as establishing standard template(s) to ensure the consistency of information reported to the DAA.

Management Comments

Partially Concurred. The DLA DIACAP Implementation Guide is being updated with a mandate to standardize DIACAP package submissions to ensure a baseline of consistency across the enterprise; the updated version of the DLA DIACAP Implementation Guide is scheduled to be staffed and coordinated within J6 no later than September 2011. However, the standardization of artifacts should be reserved on a case-by-case basis because of the overhead required to maintain and manage the standard templates. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive. Since DLA Information Operations plans to standardize the DIACAP package submissions to ensure a baseline of consistency across the enterprise, the artifacts to be uploaded in support of the C&A package should also be considered as part of the standardization process.

User Account Management

We identified deficiencies with the design and operating effectiveness of the controls related to the user account management process for EAGLE, FLIS, DMLSS-W, DSS, and EBS. The current policy and procedures did not completely address the controls required within the account management process in accordance with DLA Instruction 6402, DOD Instruction (DODI) 8500.2, and NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations." The provisioning, modification, and removal of user access was decentralized and prevented effective monitoring of user accounts by system assigned IAMs and Information Assurance Officers (IAOs). The detailed processes followed for granting, modifying, terminating, and recertifying user accounts were not documented in DLA Instruction. Consequently, each application Program Manager developed system or site-specific access control policies and procedures.

NIST Special Publication 800-53 recommended a formal access control policy that addressed purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities. NIST Special Publication 800-53 also recommended formal documented procedures to facilitate the implementation of the access control policy and associated access controls.

DLA Instruction 6402, "Information Assurance Operational Controls," required all IAOs to direct Terminal Area Security Officers to submit (e.g., DD Form 2875 (System Authorization Access Request (SAAR)), track, and manage DLA user accounts for IT systems under their purview. The Instruction further required the IAOs ensure user accounts be revalidated annually and to disable or remove user accounts that cannot be validated. In addition, DODI 8500.2 required that each IAM ensure that information ownership responsibilities were established for each DOD information system, to include accountability, access approvals, and special handling requirements. The Instruction also required a comprehensive account management process be implemented to ensure that only authorized users could gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated were promptly deactivated.

We identified the following control deficiencies related to user account management process:

- A procedure detailing the proper completion of the DOD Form 2875, SAAR, had not been developed for DLA.
- The FLIS Data Access Policy did not define the process for granting, modifying, terminating, or recertifying FLIS user accounts.
- Documentation of access authorization could not be provided for 18 of 45 FLIS users sampled.
- The EAGLE Roles Guide did not define the process for handling user transfers and terminations.
- The process for provisioning, modifying, disabling, and removing user access for DSS and EAGLE was decentralized and could not be effectively monitored by IAMs and IAOs. For example:
    - Accounts were created prior to documented approval for 10 of 45 EAGLE users sampled and the SAAR could not be provided for 1 of 45 sampled EAGLE user;
    - SAARs were not approved for access by either the Data Owner or the IAO for 19 of 45 EAGLE sampled users.
    - The DOD Office of Inspector General identified in 2009 that the DSS user profiles/functionalities were not documented and user recertification was not

  - conducted, which was confirmed when DLA Information Operations at New Cumberland was unable to provide a DSS user listing and roles listing to the audit team.
- The System Access directive for DLA Distribution and DSS did not mention when accounts should be disabled for inactivity and when they should be removed.
- The following weaknesses were identified for EBS:
  - 15 of 45 sampled users were given access to EBS before the Account Management Provisioning System (AMPS) approval date;
  - 13 of 45 sampled users that were converted from a legacy account management system did not have documentation of their current privileges;
  - Reconciliations between AMPS users, AMPS roles, and EBS were not performed.
- Annual recertification of the DMLSS-W users and roles were not being performed.

The instructions documented on the SAAR were not specific enough to ensure the proper and consistent completion of the system access requests. Additionally, adequate technical documentation for DSS, specifically for Customer Information Control System (CICS) transactions, defining DSS user profiles/functionalities was absent. Management represented that FLIS user authorization documents were scanned but not readable; therefore, they could not be provided at the time of the audit for 18 of the 45 users sampled.

Further, there was a lack of specific DLA guidance surrounding account control procedures and user recertification. Many EBS users were bulk-loaded into AMPS from the DLA legacy account management systems; therefore, the action bypassed all EBS account management controls built within the account provisioning system (AMPS). Management did not consistently enforce the usage of AMPS to request access to EBS. During the time of testing, DMLSS-W Management did not have procedures in place to recertify DMLSS-W user accounts and roles. The SAARs were inconsistently completed across DLA; therefore, security information and/or appropriate levels of approval for access to an application were not obtained. Also, the process for granting, disabling, transferring, and terminating user access was not consistently executed as intended by DLA policy. As a result, users could have had inappropriate access to DLA systems that violated segregation of duties and the principle of least privilege. Controls designed to protect DLA systems from unauthorized access to DLA sensitive logistics, payroll, and financial information that could affect the war fighters and effective stewardship of public resources were rendered ineffective.

Recommendation 16 *(Director, DLA Information Operations)*

Develop and enforce an agency-level policy and procedure for the account management process that includes the granting, modifying, terminating, and recertifying of user accounts.

Management Comments

Concurred. The Hire to Retire (H2R) Process Cycle Memorandum (PCM) describes the DLA process for employee transfers and terminations. The EAGLE Roles Guide describes EAGLE access, roles, and privileges. The DLA Finance Payroll Centers of Excellence (CoE) are responsible to add, transfer, terminate, and archive government employee records in EAGLE. Because of the restrictions and requirements already mandated by the Department Of Defense for access to local enclaves, an EAGLE user would first have to be authorized and granted access at the enclave level; a user could not access EAGLE without prior enclave access, which is controlled by site administration at each enclave. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. Management's comments did not address the development and enforcement of an agency-wide policy and procedure for account management processes. Additionally, the EAGLE Roles Guide did not reference the H2R PCM, which was a process narrative document that identified key controls. Further, the H2R PCM was not a formal policy or procedure that must be adhere to by users.

Recommendation 17 *(Director, DLA Information Operations)*

Develop and enforce the following: (a) policies and procedures for proper retention and completion of the system access authorization request that contain specific instructions, including required blocks of the form/ data fields that must be completed for each type of system access request (i.e., authorized, privileged, modification to current role, recertification, termination, etc.) and (b) a mechanism to monitor compliance with the agency-wide account management process.

Management Comments

Concurred. DLA Information Operations is planning to move the EAGLE user provisioning process to AMPS in order to process, approve, and maintain EAGLE DD Form 2875s, which will ensure standard policies and procedures are enforced. The EAGLE application team has been working with the AMPS team and DLA Finance at HQ. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. The migration of EAGLE provision process to AMPS is only a piece of the retention and completion of the system access authorization request. DLA management did not address the agency-way policies and procedures for proper retention and completion of system access authorization requests and the development of the mechanism to monitor compliance with the agency-wide account management process.

Recommendation 18 *(Director, DLA Information Operations)*

Enforce the requirement that all EBS users only be granted access or roles modified through AMPS and complete the AMPS revalidation of users converted from the legacy account provisioning application.

Management Comments

Concurred. AMPS can produce a list of known users and roles for EBS, but the administrative burden on the EBS administrators to conduct user access revalidation would be labor and time prohibitive. Additionally, this will not be necessary once all EBS users are created using AMPS. A J6 policy will be written to enforce all system access accounts be approved through AMPS. The estimated completion date for the policy is December 2012. The AMPS revalidation of users converted from the legacy account provision application is completed. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 19 *(Director, DLA Information Operations)*

Develop a process to periodically reconcile user accounts and roles within AMPS to user accounts and roles within EBS. Additionally, the process should include a reconciliation of active roles within AMPS against active roles within EBS.

Management Comments

Concurred. DLA Information Operations will develop a policy for periodic reconciliation of user accounts and roles. The estimated completion date is June 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 20 *(Director, Medical Information Management Division at DLA Troop Support)*

Enforce DLA policy for recertifying DMLSS-W users' accounts and roles on an annual basis.

Management Comments

Concurred. An annual Information Assurance (IA) review is being conducted for the DMLSS-W program. Documentation specific to access (Web Access Management SOP) will be updated to address account recertification, as well as revalidation on an annual basis. Additionally, the Information Assurance Officer is being designated as responsible for reviewing and identifying accounts. The estimated completion date is November 2011. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 21 *(Director, DLA Information Operations at New Cumberland)*

Complete the current efforts to design and document DSS user profiles that are role-based and follow the principle of least privilege. After which, management should develop a process to implement DLA policy for granting, modifying, disabling, terminating and recertifying user accounts for all DSS users.

Management Comments

Concurred. DLA Information Operations at New Cumberland had been facilitating an effort, along with other key stakeholders and users, to implement role-based access and profile realignment that will be nearing completion early next year. DLA Distribution and DLA Information Operations at New Cumberland continue to test the DLA Distribution approved DSS Role Based Access Control (RBAC) structure with DISA DECC-Mechanicsburg. RBAC and centralized account administration will comply with DLA directives to grant, modify, disable, and terminate accounts. Additionally, efforts were underway to coordinate with the DLA AMPS team to develop an automated user access revalidation tool. The DSS RBAC is scheduled to be implemented at DECC-M is December 2011 and to be implemented at DECC-Ogden by February 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 22 *(Director, DLA Information Operations at New Cumberland)*

Complete the efforts already underway to centralize the administration of DSS user provisioning, modification, disabling, and termination to enhance the oversight of user accounts by the IAO.

Management Comments

Concurred. DLA Information Operations at New Cumberland will cut over to a centralized DSS account administration methodology concurrent with the west RACF cutover. As the groundwork is in place with DSS accounts at DECC-M, final action entails re-routing DD Form 2875 requests for DSS DECC-O through the same process. The estimated completion date to implement this recommendation is November 2011. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 23 *(Director, DLA Information Operations at Ogden)*

Centralize the administration of EAGLE user provisioning, modification, disabling, and termination to enhance the oversight of user accounts by the IAO.

Management Comments

Non-Concurred. This recommendation is outside the scope of DLA Information Operations because the data is not owned by DLA Information Operations. DLA Finance Payroll Centers of Excellence (COE) are responsible for provisioning, modification, disabling, and archiving of EAGLE user accounts and are the EAGLE data owners. Subsequent to this finding, the COE's and DLA Finance met and developed a standard process for handling and administering EAGLE user accounts. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive. However, while the development of a standard process for handling and administering EAGLE user accounts as cited in management's comments was a positive enhancement, the standard procedure should be formalized and include the elements detailed in recommendation #16.

DLA Personnel Security

Evidence of users receiving appropriate verification of security clearance prior to receiving access to the EAGLE, FLIS, DMLSS-W, and EBS systems was not consistently documented. DLA field sites depended on the personnel security verification process used to grant access to DLA network instead of performing their own verifications prior to granting users access to DLA information systems. Without proper verification of personnel security, users might gain unauthorized access to sensitive government information that could harm the DLA mission.

The DODI 8500.2 stated "Individuals requiring access to sensitive information are processed for access authorization in accordance with DOD personnel security policies." In addition, the Instruction required information owners to ensure that access to all DOD information systems be granted only to appropriately cleared personnel.

We identified the following deficiencies related to personnel security control:

1. The Medical Information Management Division (MIMD) at DLA Troop Support could not provide SAARs for 41 of 45 sampled DLA Troop Support (internal users) DMLSS-W users in order to evidence users obtained appropriate background investigation or clearance prior to receiving access to DMLSS-W.

2. The MIMD at DLA Troop Support did not have a process in place to verify that users external to DLA Troop Support obtained appropriate background investigation or clearance prior to receiving DMLSS-W access.

3. The Center of Excellence for EAGLE could not provide completed SAARs for 2 of 45 sampled EAGLE users in order to evidence users obtained appropriate background investigation or clearance prior to receiving EAGLE access.

4. The DLA Logistics Information Service could not provide SAARs for 18 of 45 sampled FLIS users in order to evidence users obtained appropriate background investigation or clearance prior to receiving FLIS access.

5. The audit team did not receive evidence for 13 of 45 sampled EBS users that were converted from a legacy account management system to evidence that an appropriate background investigation or clearance information was verified prior to granting EBS access.

The MIMD at DLA Troop Support for DMLSS-W and the Center of Excellence for EAGLE relied on the personnel security verification process used to grant users access to DLA network because DMLSS-W and EAGLE users must have a DLA network account before they could access the DMLSS-W and EAGLE applications. Additionally, DMLSS-W did not have a process in place to verify background investigations and clearances for external DMLSS-W users.

Management represented that the FLIS user access authorization documents, including clearance information, were scanned but not readable; therefore, they could not be provided at the time of the audit. Also, many EBS users were bulk-loaded into AMPS from the DLA legacy account management systems; therefore, evidence of the verification of personnel security was not available. Without verifying user background investigations and clearance information, unauthorized users could have accessed sensitive government logistics and financial information that could jeopardize the war fighters' safety and DLA mission.

Recommendation 24 *(Director, DLA Information Operations)*

Develop a process for assessing and documenting the minimum background investigation and clearance requirements for all users internal to DLA.

Management Comments

Non-Concurred. DLA follows the guidance outlined in DODI 8500.02, which prescribes procedures for investigative levels of 1, 2, and 3. This instruction also prescribes procedures for applying integrated, layered protection of DOD information systems and networks. The DLA Security Representative Handbook, dated October 2008, provides additional DLA guidance to the security workforce. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. The audit testing results did not support DLA Information Operation's compliance with DODI 8500.02 for investigative levels. We modified the recommendation to include the documentation of the minimum clearance requirements for all users. Additionally, the Medical Information Management Division did not have a process in place to verify users' clearances who were external to DLA Troop Support prior to granting them access to DMLSS-W.

Recommendation 25 *(Director, DLA Information Operations)*

Incorporate the minimum personnel security requirements into a DLA access control policy and system level procedures to ensure an adequate verification of personnel security is being performed prior to granting access to DLA information systems, and as a part of the user account recertification process.

Management Comments

Concurred. DMLSS-W does not maintain security clearance documentation. This function is conducted by Base/Security Compound Office personnel. It is up to the business units to verify the need to know prior to submitting an access request. External users are not verified by DLA

Troop Support RSA Access Manager Administrators. Instead, their information is verified by each business unit for each application. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. Management's comments did not address the process DLA Information Operations will incorporate into the minimum personnel security requirements as part of the agency-wide access control policy and system level procedures to ensure a verification of personnel security is part of the process for granting users access to DLA system.

Recommendation 26 *(Director, DLA Information Operations)*

Develop a process to retain evidence for verification of personnel security requirements.

Management Comments

Concurred. The detailed corrective action plan was excluded from DLA Information Operations' formal response to the draft audit report. However, based on a follow-up communication with Management, DLA Information Operations (J65) stated that it will update the standard operating procedures on security officer procedures, to include an evidence retention process for verification of personnel security requirements with an estimated completion date of December 2012.

DLA OIG Response

Management comments were responsive.

DLA Information Assurance Awareness Training

Users internal to DLA did not consistently complete initial or refresher IA awareness training as part of the requirement to have access to DLA information systems. Users' initial and refresher IA awareness training were not consistently verified and monitored by management to ensure training was taken in accordance with DLA policy. As a result, users may have performed inappropriate or unsafe activities while using DLA systems that could have exposed the agency to cyber attacks and threatened the integrity, availability, and confidentiality of DLA sensitive data.

One element of having a successful IA program was an effective security training and awareness strategy. Public Law 100-235 (The Computer Security Act of 1987) required that all users of government computers received annual computer security awareness training. Additionally, DODI 8500.2 required that all DOD employees and IT users maintain a degree of understanding of IA policies and doctrine commensurate with their responsibilities. The Instruction also required that they be capable of appropriately responding to and reporting suspicious activities and conditions, and that they know how to protect the information and IT they access. To achieve this understanding, all DOD employees and IT users were required to receive both initial and periodic refresher IA training.

We identified the following inconsistencies related to the completion of the initial and refresher IA Awareness training for users internal to DLA:

- Initial and refresher IA awareness training was not monitored by the Information Assurance Managers for DSS, EAGLE, FLIS, and DMLSS-W users internal to DLA.
- Evidence for completion of initial or refresher IA awareness training for internal users could not be provided for 22 of 45 EAGLE users sampled and for 43 of 45 DMLSS-W users sampled.
- 7 of 45 sampled internal EBS users did not have evidence of initial or refresher IA awareness training information prior to being granted access or retaining access to the system.

Information system users who had access to critical DLA information systems may not have been trained on the information technology security policy and procedures. Also, DLA Information Operations Management did not have a monitoring process to ensure that users received and completed the initial and periodic refresher IA training prior to having access to DLA information systems or to retain their access to the systems. As a result, system users may not have known the appropriate actions to respond and report suspicious activities and conditions so DLA Information Operations could quickly contain security threats and protect the sensitive information and information technology.

Recommendation 27 (*Director, DLA Information Operations)*

Develop a process to ensure that all users internal to DLA complete IA awareness training prior to access being granted to DLA systems, and enforce IA awareness refresher training for users internal to DLA as a condition of continued access to DLA information systems.

Management Comments

Non-Concurred. DLA Information Operations (J6) had processes in place requiring periodic and initial user IA Awareness training that was executed at the J6 Field Site/PMO and business area level. IA training completion was verified prior to granting access to any DLA Network through the System Authorization Access Request process via a DD Form 2875. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were nonresponsive. Our test results identified users with access to DLA systems without evidence of a completed initial or refresher IA awareness training.

External DLA System Users

We observed that program managers of the five selected AIS applications inconsistently classified the users external to DLA and managed the IA awareness training and security verification requirements for the defined external users differently. Refer to Table 4 below for a comparison among the five selected AIS applications.

Table 4. Definition of Internal & External Users to DLA Systems

System Name	Internal User Definition	External User Definition	IA Awareness Training Verification Process	Personnel Security Clearance Verification Process
EAGLE	Not defined.	Not defined.	A process has been developed for DLA users only.	A process has been developed for DLA users only.
FLIS	Located at the Battle Creek, MI facility.	Not located at the Battle Creek, MI facility.	A process has been developed for internal users only.	A process has been developed for Department of Defense users only.
DMLSS-W	DLA employee or contractor.	Non - DLA employee or contractor.	A process has been developed for internal users only.	A process has been developed for internal users only.
DSS	Not defined.	Not defined.	A process has been developed for DLA users only.	A process has been developed for DLA users only.
EBS	Not defined.	Not defined.	A process has been developed for DLA users only.	A process has been developed for DLA users only.

Source: DLA OIG Developed

System users categorized as external to DLA were not required to provide evidence of recent completion (i.e., within the last 12 months) of IA awareness training and evidence that an appropriate background investigation or clearance had been completed prior to receiving access to DLA systems.

DODI 8500.2 required all DOD employees and IT users to maintain a degree of understanding of IA policies and doctrine commensurate with their responsibilities. The Instruction also required that they be capable of appropriately responding to and reporting suspicious activities and conditions, and they know how to protect the information and IT they access. To achieve this understanding, all DOD employees and IT users were supposed to receive both initial and periodic refresher IA training. Additionally, individuals requiring access to sensitive information should be processed for access authorization in accordance with DOD personnel security policies and the information owners were responsible for ensuring that access to all DOD information systems were granted only to appropriately cleared personnel.

DLA Information Operations had not developed an agency-wide policy and procedure requiring program managers to document a definition of users who constituted internal and external to DLA and the associated IA awareness training and the level of security clearance verification requirements to have access to DLA systems. As a result, users may have had access to DLA systems that had not been properly trained on IA awareness and/or been properly cleared through completion of a background investigation that could have negatively affected the confidentially, integrity and availability of DLA systems.

Recommendation 28 *(Director, DLA Information Operations)*

Develop a policy and procedure requiring a definition of what constitutes an internal and external user to DLA for each system. In addition, document in the system access policy for each DLA system the IA awareness training and security clearance verification requirements for the defined internal and external users.

Management Comments

Concurred. DLA Information Operations (J64) has drafted a DLA Instruction, Enterprise Remote Access Policy and Procedures. This draft DLA Instruction does not currently address internal or external users but will be modified to include definitions of both. The estimated completion date is June 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

IV. DLA ENERGY NOTICE OF DEFICIENCY VALIDATION

DLA Information Operations at Fort Belvoir had made some progress in addressing the deficiencies identified within the DLA Energy FISCAM Readiness Assessment Report, dated June 1, 2007. Specifically, DLA Information Operations at Fort Belvoir had included the Requirements Manager (RM) application as part of the Headquarter Information Technology System (HQITS) enclave accreditation boundary, and was certified and accredited in accordance with the relevant DLA, DOD, NIST, and OMB Guidance, as recommended within NOD 8 and received an authorization to operate on January 12, 2010. However, DLA Information Operations at Fort Belvoir had not fully addressed the deficiencies identified within NOD 9, 18, and 19. Please refer to Table 6 for the summary of the status of the identified deficiencies.

Table 6: Summary of the Status of the Identified Deficiencies

NOD #	Description	Summary of Required Actions	Deficiency Status
8	Certification and accreditation of the Requirements Manager system	1. Certify and accredit RM application and general support system	Remediated
9	Centralized management of plan of action and milestones (POA&M)	1. Implement a DLA centralize POA&M process	Not Fully Remediated *(Refer to POA&M Management deficiency in section 2 of the report)*
		2. Update POA&M policies and procedures to include steps on how to close POA&Ms	Not Fully Remediated *(Refer to POA&M Management deficiency in section 2 of the report)*
		3. Track and monitor POA&Ms across the DLA Information Operations field sites	Remediated
18	Access and security control information within the certification and accreditation package	1. Update the BSM-E, PORTS, and DFAMS security documents to include a overview of the security controls	Remediated
		2. Update the BSM-E, PORTS, and DFAMS security documents to include details on the security controls (e.g. available access functions, description of the functions, and combination of functions that users can and cannot have)	Not Fully Remediated
		3. Update the BSM-E, PORTS, and DFAMS security documents to include application and system software documentation regarding segregation of duties, as well as formally defining all available roles	Not Fully Remediated
19	Continuity of operations planning, training, and testing	1. Update the DFAMS and DISA DECC Ogden Contingency Plans to include the current data center environment controls and training requirements	Not Fully Remediated
		2. Update the [HQITS] Contingency Plan to include the RM Application	Not Fully Remediated
		3. Perform a BSM-E COOP Test exercise to include the applications and systems that the exercise covers. Ensure that the COOP testing covers BSM-E subsystems, PORTS, and [HQITS].	Not Fully Remediated
		4. Update the DFAMS contingency plan to include the restoration and testing of backup tapes procedures	Remediated

Source: DLA OIG Developed

The deficiencies identified within NOD 9 were reported as part of the POA&M management process deficiency under section 2 of this report related to the DLA implementation of the DIACAP. The following section addressed the updated condition and recommendations to address deficiencies identified as part of NOD 18 and 19.

Segregation of Duties

We determined that security controls around the Paperless Ordering and Receipt Transaction Screens (PORTS) had been integrated into the BSM-E C&A package and that the BSM-E and DFAMS C&A package included artifacts in eMASS for the IA control on Functional Architecture Documentation, which provided an overview of the security controls for the systems. Also, DLA Information Operations at Fort Belvoir had implemented mitigating controls by monitoring sensitive system roles for BSM-E and DFAMS. However, the segregation of duties deficiencies identified within NOD 18 for BSM-E and DFAMS had not been fully remediated. Documenting the system roles and potential incompatibilities for BSM-E, DFAMS, and PORTS within the technical documentation was not considered during the system development or sustainment phases of the system lifecycle. As a result, inappropriate access and modification of DLA fuel and financial data may not be prevented by the systems, which could negatively affect data confidentiality and integrity.

DOD Directive 8500.01 required that information assurance requirements be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DOD information system in accordance with 10 United States Code, Section 2224, Office of Management and Budget Circular A-130, Appendix III, DOD Directive 5000.1, and other IA-related DOD guidance. Also, DODI 8500.2 required that access to all DoD information was determined by both its classification and user need-to-know. Need-to-know was established by the Information Owner and enforced by discretionary or role-based access controls. Access controls were established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified.

Based on testing performed, DLA Energy did not have detailed listings of the available functions/roles for BSM-E and PORTS. Additionally, listings of the permissible/not-permissible combination of functions/roles for BSM-E, PORTS, and DFAMS had not been developed, documented, and designed for the systems. Also, as part of a modernization project, DLA Energy was developing Energy Convergence, which was a project within EBS to replace several DLA Energy systems, including BSM-E and DFAMS. Management represented that the Energy Convergence project would address deficiencies in the area of segregation of duties identified as within NOD 18.

As part of the development of the Energy Convergence system, DLA Information Operations at Fort Belvoir had been focusing its resources on the development of the new system instead of updating documentation for the sun-setting systems. Without detailed listings of the available functions/roles and permissible/not permissible combination of functions/roles for BSM-E, PORTS, and DFAMS, DLA Energy Management could not adequately implement the concept of segregation of duties or adequately design the system controls to prevent users from performing incompatible duties. Consequently, users might perform functions outside of their assigned tasks and negatively affect the DLA Energy missions and business functions, which would lead to ineffective management of fuels for the war fighters and improper financial reporting.

Recommendation 29 *(Director, DLA Information Operations at Fort Belvoir)*

Coordinate with the subject matter experts to establish listings of available user functions/roles for BSM-E and PORTS.

Management Comments

Concurred. DLA Information Operations at Fort Belvoir will work with DLA Energy to ensure that the recommendations are addressed in the Energy Convergence (EC) Program Office. The estimated completion date is June 2014. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 30 *(Director, DLA Information Operations at Fort Belvoir)*

Coordinate with the subject matter experts to establish listings of the permissible/not-permissible combination of functions/roles for BSM-E, PORTS, and DFAMS.

Management Comments

Concurred. DLA Information Operations at Fort Belvoir will work with DLA Energy to ensure that the recommendations are addressed in the Energy Convergence (EC) Program Office. The estimated completion date is June 2014. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 31 *(Director, DLA Information Operations at Fort Belvoir)*

Ensure the established listings of available user functions/roles and permissible/not permissible combination of functions/roles that are critical to protecting DLA Energy systems be incorporated into the Energy Convergence system requirements and system documentation.

Management Comments

Concurred. DLA Information Operations at Fort Belvoir will work with DLA Energy to ensure that the recommendations are addressed in the Energy Convergence (EC) Program Office. The estimated completion date is June 2014. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Disaster Recovery/Continuity of Operations Planning Training

We identified that the DFAMS continuity exercise conducted from March 15, 2010 through April 2, 2010, and the BSM-E continuity exercise conducted from July 19, 2010 through July 23, 2010, included establishing network connectivity between select users and the DISA alternate recovery site in Mechanicsburg, PA and batch processing of transactions. However, deficiencies in the area of Continuity of Operations (COOP) training and the COOP documentation for RM (now residing under the Headquarter Information Technology System (HQITS) enclave), BSM-E, and DFAMS identified as part of the NOD 19 had not been fully remediated. DLA Information Operations had not developed a formal COOP training program for recovery and response team personnel across the DLA enterprise to enforce the Disaster Recovery/COOP training outlined in DLA Instruction 6104, "Information Technology COOP." As a result, COOP team personnel may not know how to respond in the event of a catastrophic failure at the primary system processing facility.

NIST Special Publication 800-34 "Contingency Planning Guide for Federal Information Systems" required organizations to train personnel in their contingency roles and responsibilities with respect to the information system and provide refresher training. Training for personnel with continuity plan responsibilities should complement testing. Training should be provided at least annually and new hires who had plan responsibilities should have received training shortly after they were hired. Ultimately, contingency plan personnel should be trained to the extent that they were able to execute their respective recovery procedures without aid of the actual plan document. This was an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the disaster. In addition, DLA Instruction 6104 required that all Recovery and IT COOP team members received proper training commensurate with their assigned roles and responsibilities. At a minimum, this included the annual COOP awareness training for all resources and recovery procedures for the recovery team members.

Based on testing performed, the COOP Plans for HQITS, BSM-E, and DFAMS did not contain information on a formal Disaster Recovery/COOP training program. Additionally, the HQITS COOP Plan did not list RM as one of the covered systems even though RM was part of the HQITS enclave accreditation boundary. Management relied on annual IA Awareness training and the execution of COOP exercises as a method to increase COOP awareness for DLA personnel, instead of establishing a formal Disaster Recovery/COOP training program. The HQITS COOP Plan did not list RM as one of the covered systems due to a lack of management oversight. Consequently, the DLA Energy systems may not have been able to perform DLA Energy inventory and financial functions to support DLA mission in an event of a catastrophic failure of the primary processing facility. Additionally, without the inclusion of RM under the HQITS COOP Plan, RM data may not have been available in a timely manner to support DLA Energy operations.

Recommendation 32 *(Director, DLA Information Operations)*

Establish a formal Disaster Recovery/COOP Training Program across the DLA Enterprise.

Management Comments

Partially Concurred. DLA Enterprise Disaster Recovery/COOP Training Program was established September 2010. The draft IT COOP Instruction includes this training requirement. Additionally, the DLA HQ IT and HQ Business COOP Team has joined with the FEMA Team to offer formal Disaster Recovery/COOP training to site COOP coordinators and Planners. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation 33 *(Director, DLA Information Operations at Fort Belvoir)*

Identify all supported systems, including RM, under the HQITS COOP Plan.

Management Comments

Partially Concurred. The current HQITS IT COOP Plan (April 2011) included the RM system. Verbatim management comments can be found in Appendix J.

DLA OIG Response:

Management comments were responsive. However, the HQITS IT COOP Plan should be updated to include the RM system and all other systems supported by the HQITS enclave.

OTHER OBSERVATION

During the audit, the audit team observed a potential risk in the area of Rules of Behavior. This control was being performed at the enclave level for DLA information systems, which was outside the identified information assurance controls tested for the selected five AIS applications. Specifically, the process for completing and maintaining user acknowledgement of the DLA Rules of Behavior was not consistently followed and understood. External users to

DLA were not required to acknowledge the Rules of Behavior prior to receiving access to the DMLSS-W, EAGLE, and FLIS applications. Additionally, internal users' acknowledgements of the rules of behavior were not consistently retained by DLA Information Operations.

CONCLUSIONS

Based on the results of audit testing, DLA generally complied with the requirements for the FISMA reporting process. However, we issued one recommendation related to the retention of supporting data used for FISMA reporting at DLA Information Operations, as part of the data collection process in order to enhance the effectiveness of the reporting process. A summary of this recommendation can be found in Appendix A.

Additionally, we determined that DLA generally did not implement the DIACAP in accordance with DODI 8510.01. We identified three control deficiencies related to the DLA implementation of DIACAP and 10 recommendations issued to the Director of Information Operations to improve the maturity level of DLA C&A process. A summary of these recommendations can be found in Appendix A.

Further, we concluded that 10 of 28 high-impact IA controls generally were not designed and/or operated effectively in accordance with DOD Directive 8500.01E and DODI 8500.2 for five selected DLA AIS applications. DLA Office of the Inspector General Audit Division (OIG), made 34 recommendations to management in order to improve the design and operating effectiveness of the selected IA controls. Of the 34 recommendations to management, 17 recommendations resulted in enterprise-level findings and 17 recommendations resulted in system-specific findings. A summary of these recommendations can be found in Appendix A and E through I.

Through our validation of the corrective actions related to deficiencies identified as part of the DLA Energy FISCAM Readiness Assessment Report, NOD 8, 9, 18, and 19, DLA OIG verified that 1 of 4 deficiencies was fully remediated. We issued five recommendations as a result of the validation of corrective actions related to NOD 9, 18, and 19 directed to the Director of DLA Information Operations and Director of Information Operations at Fort Belvoir. A summary of these recommendations can be found in Appendix A.

In addition, during our fieldwork, we identified one observation regarding the control related to the Rules of Behavior that merits management's attention in order to improve the security of DLA Information systems.

SUMMARY OF RECOMMENDATIONS

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
1	Develop policy and procedure for the retention of supporting data used for FISMA reporting.	Director, DLA Information Operations	Completed	November 2010
2	Update and enforce the validation process to assess and document the design/operating effectiveness of all IA controls for DLA systems.	Director, DLA Information Operations	Non-Concurred	Not Applicable
3	Re-evaluate all applicable IA controls and confirm the correct assignment of inherited, shared, and DLA-owned baseline IA controls for each DLA system in eMASS.	Director, DLA Information Operations	Open	To Be Determined
4	Enforce the requirement that a program or system manager be designated for each DLA system and who will perform the functions as described in accordance with DODI 8510.01 and DLA DIACAP Implementation Guide.	Director, DLA Information Operations	Completed	September 2011
5	Coordinate with the Director of DLA or obtain the delegation of authority to update the DLA ESSD and SLAs with DISA to explicitly define the expected level of services and IA roles and responsibilities.	Director, DLA Information Operations	Open	December 2012
6	Coordinate with DISA to explicitly define listings of system-specific inherited, shared, and customer-owned IA controls for all DISA-hosted DLA systems.	Director, DLA Information Operations	Open	December 2012

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
7	Communicate guidance to the Director of DLA Information Operations at Ogden on the minimum information that must be reviewed and communicated back to DLA Information Operations to update the SLAs with DISA on an annual basis.	Director, DLA Information Operations	Open	December 2012
8	Update the DLA DIACAP Implementation Guide to provide detail instructions on the standard format and appropriate artifacts in support of the residual risk analysis for IT security weaknesses reported on the POA&Ms.	Director, DLA Information Operations	Non-Concurred	Not Applicable
9	Implement an enterprise procedure for disseminating, tracking, and managing DLA IT security weaknesses identified as the result of internal or external assessments or audits (i.e., IA security assessments during the C&A process, annual system security review, DLA OIG audits, GAO audit, and DOD IG audits).	Director, DLA Information Operations	Non-Concurred	Not Applicable
10	Develop and implement a process for validating evidence that corrective actions for security weaknesses have been fully resolved and the corrective actions have been tested for the deficiencies before marking POA&Ms as "Completed."	Director, DLA Information Operations	Non-Concurred	Not Applicable
11	Coordinate with DISA to obtain validation test results and applicable supporting artifacts for inherited IA controls.	Director, DLA Information Operations	Completed	November 2011

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
12	Designate viable alternate system recovery site(s) for EAGLE and DMLSS-W, update COOP documentation, and perform COOP testing. In the interim: 1. Create a POA&M in order to establish and implement mitigating controls until designated alternate system recovery site(s) are established, such as selecting temporary system recovery site(s); 2. Provide an estimated timeline to have designated alternate system recovery site(s) in place and operational; and 3. Update COOP documentation for each system to reflect the designated alternate system recovery site(s), the correct MAC level, and perform COOP testing using the recovery site(s).	Director, DLA Information Operations	Open	March 2012

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
13	Implement activities to improve the viability of EBS alternate system recovery site. For example, • Update the Certification and Accreditation documentation in eMASS to accurately reflect the designation of the DISA, Mechanicsburg, PA facility as the alternate recovery site; • Complete the coordination with the key stakeholders and user representatives to develop a Business Impact Analysis document and to create and/or update a business continuity-planning document and the IT continuity plan; and • Ensure the completion of an upgrade to the backup and recovery infrastructure at DISA facility in Mechanicsburg, PA in order to meet future requirements.	Director, DLA Information Operations	Completed	September 2011
14	Establish, at a minimum, a list of supporting documentation or artifacts that are required as part of the DLA system certification process (i.e., system-level or IA control-specific artifact) to meet OMB Circular A-130 requirement for a SSP.	Director, DLA Information Operations	Non-Concurred	Not Applicable
15	Standardize the required artifacts in support of the C&A process, such as establishing standard template(s) to ensure the consistency of information reported to the DAA.	Director, DLA Information Operations	Completed	September 2011

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
16	Develop and enforce an agency-level policy and procedure for the account management process that include the granting, modifying, terminating, and recertifying of user accounts.	Director, DLA Information Operations	Open	December 2012
17	Develop and enforce the following: (a) policies and procedures for proper retention and completion of the system access authorization request that contain specific instructions, including required blocks of the form/data fields that must be completed for each type of system access request (i.e., authorized, privilege, modification to current role, recertification, termination, etc.) and (b) a mechanism to monitor compliance with the agency-wide account management process.	Director, DLA Information Operations	Open	December 2012
18	Enforce the requirement that all EBS users only are granted access or current roles be modified through AMPS and complete the AMPS revalidation of users converted from the legacy account provisioning application.	Director, DLA Information Operations	Open	December 2012
19	Develop a process to periodically reconcile user accounts and roles within AMPS to user accounts and roles within EBS. Additionally, the process should include a reconciliation of active roles within AMPS against active roles within EBS.	Director, DLA Information	Open	June 2012

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
20	Enforce DLA policy for recertifying DMLSS-W user's accounts and roles on an annual basis.	Director, Medical Information Management Division at DLA Troop Support	Completed	November 2011
21	Complete the current efforts to design and document DSS user profiles that are role-based and follow the principle of least privilege. After which, management should develop a process to implement DLA policy for granting, modifying, disabling, terminating and recertifying user accounts for all DSS users.	Director, DLA Information Operations at New Cumberland	Open	February 2012
22	Complete the efforts already underway to centralize the administration of DSS user provisioning, modification, disabling, and termination to enhance the oversight of user accounts by the IAO.	Director, DLA Information Operations at New Cumberland	Completed	November 2011
23	Centralize the administration of EAGLE user provisioning, modification, disabling, and termination to enhance management oversight of user accounts by the IAO.	Director, Information Operations at Ogden	Non-Concurred	Not Applicable
24	Develop a process for assessing and documenting the minimum background investigation and clearance requirements for all users internal to DLA.	Director, DLA Information Operations	Non-Concurred	Not Applicable

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
25	Incorporate the minimum personnel security requirements into a DLA access control policy and system level procedures to ensure an adequate verification of personnel security control is being performed prior to granting access to DLA information systems and as a part of the user account recertification process.	Director, DLA Information Operations	Completed	November 2011
26	Develop a process to retain evidence for verification of personnel security requirements.	Director, DLA Information Operations	Open	December 2012
27	Develop a process to ensure that all users internal to DLA complete IA awareness training prior to access being granted to DLA systems, and enforce IA awareness refresher training for users internal to DLA as a condition of continued access to DLA information systems.	Director, DLA Information Operations	Non-Concurred	Not Applicable
28	Develop a policy and procedure requiring a definition of what constitutes an internal and external user to DLA for each system. In addition, document in the system access policy for each DLA system the IA awareness training and security clearance verification requirements for the defined internal and external users.	Director, DLA Information Operations	Open	June 2012
29	Coordinate with the subject matter experts to establish listings of available user functions/roles for BSM-E and PORTS.	Director, DLA Information Operations at Fort Belvoir	Open	June 2014

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
30	Coordinate with the subject matter experts to establish listings of the permissible/not-permissible combination of functions/roles for BSM-E, PORTS, and DFAMS.	Director, DLA Information Operations at Fort Belvoir	Open	June 2014
31	Ensure the established listings of available user functions/roles and permissible/not permissible combination of functions/roles that are critical to protecting DLA Energy systems be incorporated in the Energy Convergence system requirements and system documentation.	Director, DLA Information Operations at Fort Belvoir	Open	June 2014
32	Establish a formal Disaster Recovery/COOP Training Program across the DLA Enterprise for recovery team personnel.	Director, DLA Information Operations	Open	June 2012
33	Identify all supported systems, including RM, under the HQITS COOP Plan.	Director, DLA Information Operations at Fort Belvoir	Completed	April 2011

Appendix B

ABBREVIATIONS USED IN THIS REPORT

AIS	Automated Information System
AMPS	Account Management Provisioning System
ATO	Authorization To Operate
BSM-E	Business Systems Modernization - Energy
C&A	Certification and Accreditation
CA	Certification Authority
CAC	Common Access Card
CAT	Category
CCB	Configuration Control Board
CICS	Customer Information Control System
CL	Confidentiality Level
CM	Configuration Management
COE	Center of Excellence
COOP	Continuity of Operations
COTS	Commercial-Off-The-Shelf
DAA	Designated Accrediting Authority
DECC	Defense Enterprise Computing Center
DFAMS	Defense Fuel Automated Management System
DIACAP	DOD Information Assurance Certification and Accreditation Process
DIBBS	DLA Internet Bid Board System
DISA	Defense Information Systems Agency
DITPR	DOD Information Technology Portfolio Repository
DMLIIS	Defense Medical Logistics Items Identification System
DMLSS-W	Defense Medical Logistics Standard Support Wholesale
DOD IG	DOD Inspector General
DODI	Department of Defense Instruction
DOE	DLA Ogden Enclave
DPACS	DLA Pre-Award Contracting System
DSS	Distribution Standard System
EAGLE	Employee Activity Guide Labor Entry
EBS	Enterprise Business System
E-Convergence	Energy Convergence
eMASS	Enterprise Mission Assurance Support System
ERP	Enterprise Resource Planning
ESSD	Enterprise Service Support Document
FISCAM	Federal Information System Controls Audit Manual

FISMA	Federal Information Security Management Act
FLIS	Federal Logistics Information System
FOUO	For Official Use Only
FTP	File Transfer Protocol
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GOTS	Government Off The Shelf Software
HQC	Headquarters Complex
HQITS	Headquarters Information Technology System
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IBM	International Business Machines
ID	Identification
IG	Inspector General
KS	Knowledge Service
MAC	Mission Assurance Category
MedPDB	Medical Product Databank
MIMD	Medical Information Management Division
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NOD	Notice of Deficiency
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
PII	Personally Identifiable Information
PIN	Personal Identification Number
PLFA	Primary Level Field Activity
POA&M	Plan of Action and Milestone
PORTS	Paperless Ordering and Receipt Transaction Screens
PR	Problem Report
QA	Quality Assurance
RACF	Resource Access Control Facility
RM	Requirements Manager
SAAR	System Authorization Access Request
SAP	Systems Applications and Products
SCA	System Change Administrator
SCR	System Change Request
SDE	Service Desk Express
SDLC	Software Development Life Cycle
SIP	System Identification Profile
SLA	Service Level Agreement

SRVA	Supplier Requirements Visibility Application
SSP	System Security Plan
TASO	Terminal Area Security Officer
TOWS	Task Order Website
TSS	Top Secret Security
VSTS	Visual Studio Team System

Appendix C

ACKNOWLEDGMENTS

Auditors:
Trang Ho, IT AuditManager, DLA Office of the Inspector General Audit Division
Alice Nguyen, IT Audit Manager, DLA Office of the Inspector General Audit Division
Wen-Tswan Chen, IT Auditor, DLA Office of the Inspector General Audit Division
Sunlon Oeung, IT Auditor, DLA Office of the Inspector General Audit Division
Edward Bailey, IT Auditor, DLA Office of the Inspector General Audit Division

Appendix D

DETAIL AUDIT SCOPE AND METHOLOGY

The DLA Implementation Guide established and prescribed DLA process for the implementation of the DIACAP, which established a net-centric C&A process for authorizing the operating of all DLA information systems. The required DLA C&A process was consistent with the FISMA, DOD Directive 8500.01E and the DODI 8510.01 requirements. The DIACAP Knowledge Service (KS) was one of the approved resources for Information Assurance (IA) personnel to use for performing C&A on a system and was the DOD official website for department level DIACAP policy and implementation guidance.

This audit focused on five DLA owned unclassified Automated Information System (AIS) applications with the following criteria:

- Mission Assurance Category (MAC) Level: III
- Confidentiality Level: Sensitive
- Judgmentally selected high-impact IA controls
- Excluding:
  - Personally identified information
  - Physical security and environmental
  - Enclave boundary defense

Based on information from the DIACAP KS for MAC III and Confidentiality Level- Sensitive systems, excluding Physical and Environmental Controls and Enclave Boundary Defense subject areas, 28 high-impact IA controls were selected. The subject areas were limited to Continuity, Security Design and Configuration, Enclave Computing Environment, Identification and Authentication, and Personnel. Refer to Table 7 below for the specific 28 high-impact IA controls and related sub-controls selected for this audit:

Table 7. Listing of 28 High-Impact IA Controls

Control ID		Description of IA Control
1	COBR 1-1, 1-2, 1-3	Protection of Backup and Restoration Assets, Physical Security Controls & Technical Security Controls.
2	COSW 1-1	Software Backup.
3	COTR 1-1	Trusted Recovery.
4	DCAS 1-1, 1-2	GOTS Product Evaluation and COTS Product Evaluation.
5	DCCS 1-1	Configuration of newly acquired IA and IA-enabled products is carried out in accordance with non-DoD standards (e.g., SANS, ICSA, Vendors) where DoD standards are not available.
6	DCHW 1-1, 1-2	HW Baseline – Inventory Maintenance, HW Baseline – Backup Copy of Inventory.
7	DCID 1-2	Interconnection Documentation – AIS Application.
8	DCIT 1-1	IA for IT Services.
9	DCPR 1-1	Configuration Management Process.
10	DCSD 1-1, 1-2	IA Documentation – System Security Documentation, IA Documentation – Appointments.
11	DCSR 2-1	Specified Robustness – Medium.
12	DCSS 1-1	System State Changes – Shutdown and Initialization.
13	DCSW 1-1, 2-1	Software Baseline - Inventory, Software Baseline - Inventory Backup.
14	ECAN 1-1, 1-2, 1-3	Access for Need-to-Know: Discretionary Access Controls.
15	ECLP 1-1, 1-2	Non-Privileged Accounts for Privileged Users.
16	ECML 1-1	Marking and Labeling for AIS Applications.
17	ECPA 1-1	Privileged User Access Assignment based on a Role-Based Access Scheme.
18	ECSC 1-1	Security Configuration Compliance.
19	ECTC 1-1	Tempest Controls.
20	ECVP 1-1	Virus Protection.
21	ECWN 1-1	Wireless Policy Compliance.
22	IAAC 1-1, 1-2, 1-3, 1-4	Consistent Account Management, Suspended User IDs and Passwords, Removal of User IDs.
23	IAIA 1-1, 1-2, 1-3, 1-4, 1-5, 1-6, 1-7, 1-8, 1-9, 1-10, 1-11	Individual Identification and Authentication.
24	PRAS 1-1	Access to Sensitive Information.
25	PRMP 1-1, 1-2	Maintenance Personnel, Sensitive Systems – Authorized Personnel, Processes in Place for Determining Authorized Maintenance Personnel.
26	PRNK 1-1	Need-to-Know Access.
27	PRRB 1-1	System Rules of Behavior.
28	PRTN 1-1, 1-2	Training – Roles and Responsibilities, Training – IA Awareness.

Source: DLA OIG Developed

To verify the design and operating effectiveness of the high-impact IA controls and DLA Implementation of the DIACAP, we judgmentally selected the following five AIS applications:

- **Employee Activity Guide for Labor Entry (EAGLE)** was a DLA time and attendance / workload and project tracking system that provided management with an automated tool to collect data for analysis, planning, and statistical reporting, which was also used to prepare civilian employee time and attendance records. EAGLE was comprised of multiple web servers.

- **Federal Logistics Information System (FLIS**) was the largest logistics information database in the world. Its mission was to provide information support for all logistics disciplines worldwide. It was a mainframe-based application, operating on a zOS system. FLIS cataloged government materiel that was repetitively procured, stocked and issued as to each item's characteristics, source, and management as an Item of Supply.

- **Defense Medical Logistics Standard Support Wholesale (DMLSS-W)** was the standard DOD medical logistics system enabling health care providers to deliver cost-effective, state-of-the-art healthcare to patients worldwide. DMLSS-W/DMMOnline was a web portal with web-based publishing with limited query capabilities. The DMLSS-W system was comprised of web servers, authentication servers, and database servers.

- **Distribution Standard System (DSS)** was the integrated core warehousing and traffic management system. It was a mainframe-based application, operating on an OS/390 system. DSS was comprised of over 72 database tables and stored millions of records containing active and historical information applying to the receipt, storage, and shipment of material for the purposes of supporting the DOD, DLA, and DDC logistics mission.

- **Enterprise Business System (EBS)** was a DLA Enterprise software suite that utilized leading edge technology to support supply chain management and core business modules that included: Procurement, Order Management, Inventory Management, Technical Quality, and Finance. EBS was comprised of a robust COTS-based Enterprise Resource Planning (ERP) system operating on the SAP platform.

The following systems were reviewed in order to validate the corrective actions related to NOD 8, 9, 18, and 19, issued as part of the FISCAM Readiness Assessment Report dated, June 1, 2007:

- **Business Systems Modernization-Energy (BSM-E)** was an integrated system of systems using an open system architecture design. BSM-E provided an automated, integrated, and responsive system for managing all DOD fuels. The Enterprise Level managed procurement, supply, and financial functions for DLA Energy. BSM-E was a multi-functional AIS that processed point of sale data and provided inventory control, finance and accounting, procurement, and facilities management. BSM-E was composed of an integrated set of Commercial-Off-The-Shelf (COTS) software applications and hosted on commercially available computer hardware. The Paperless Ordering and Receipt Transaction Screens (PORTS) had been integrated into the BSM-E C&A package.

- **Defense Fuels Automated Management System (DFAMS)** provided an automated, integrated, and responsive system for managing the procurement, storage, and use of bulk fuel and other petroleum products by DOD agencies and service components.

- **Headquarter Information Technology System (HQITS)** –HQITS was classified as an enclave. An Internet Protocol routed network that served the McNamara Headquarters Complex (HQC) located on Fort Belvoir, Virginia. The Requirements Manager (RM) application was included as part of the HQITS accreditation boundary.

To accomplish the audit objectives, we performed the following procedures:

- Reviewed prior external and internal audit and assessment reports, DOD issuances, the Federal Information Security Management Act of 2002; OMB and DOD Fiscal Year 2010 FISMA reporting guidance; and OMB Circulars.
- Reviewed security documentation in support of IA controls.
- Interviewed EAGLE, FLIS, DMLSS-W, DSS, EBS, BSM-E, DFAMS, and HQITS IA personnel.

We used the following sampling methods to test the selected design and operating effectiveness of IA controls:

1. Random interval record sampling of 45 records using an audit analytical tool, called ACL that systematically picked the random starting point and random selection interval based on a random seed created by the utility, which ensured each item had an equal opportunity of being selected thereby preventing auditor's bias. This methodology was used to select the following samples:
    a. DSS account management process for DSS Western Region using a population of 102 active users as of February 3, 2011.
    b. FLIS account management process using a population of 144 active users with a creation date of September 21, 2009 to December 13, 2010.
    c. EAGLE account management process, IA awareness training, and personnel security using a population of 15,703 active users with a creation date from April 16, 2009 to January 20, 2011.

2. Random sampling using the random number generator in Microsoft Excel to create a random value with a fixed interval, which was then sorted from smallest value to largest value in order to identify 45 items for sample testing. This methodology was used to select the following samples:
    a. EBS account management process, IA awareness training, and personnel security, using a population of 14,126 active users as of January 3, 2011.
    b. DMLSS-W account management process for users internal to DLA using a population of 2,873 active users with a creation date from March 29, 2010 to November 1, 2010.
    c. FLIS Configuration Management (CM) process using a population of 116 system changes moved to production from August 30, 2009 to September 30, 2010.

d. DMLSS-W CM process using a population of 115 system changes moved to production from September 1, 2009 to September 30, 2010.
e. EBS CM process using a population of 3,648 system changes moved to production during fiscal year 2010.

3. Judgmental sampling through manual selection by auditors using defined criteria for a selection of sample items. A listing of samples using this method is detailed below:
   a. 8 of 39 employees/contractors for FLIS terminated from a population of terminated employees/contractors listing as of November 29, 2010.
   b. All 45 DMLSS-W internal users to DLA from the period of March 29, 2010 to November 1, 2010 for IA awareness training testing and background and clearance testing.
   c. All 43 system changes from DSS from November 6, 2009 to September 30, 2010.

Additionally, the DLA OIG audit team obtained information from the sites listed below. Refer to table 8 below for the list of sites where the sources of the information was obtained and the associated audit objectives.

Table 8. List of Sites with Associated Audit Objectives

	Audit Objectives			
Sites Where the Sources of the Information Were Obtained	FISMA Reporting Process	DLA Implementation of DIACAP	Design and Operating Effectiveness of IA Controls for Selected Systems	Validation of Corrective Actions for DLA Energy Systems
DLA Information Operations Headquarters, Fort Belvoir and/or Alexandria, VA	x	x	x	x
DLA Information Operations at Philadelphia, PA			x	
DLA Troop Support, Philadelphia, PA		x	x	
DLA Information Operations at New Cumberland, PA		x	x	
DLA Information Operations at Columbus, OH			x	
DLA Information Operations at Ogden, UT (New Cumberland Office)		x	x	
DLA Defense Logistics Information Service at Battle Creek, MI		x	x	
DLA Information Operations at Richmond, VA			x	
DLA Information Operations at Fort Belvoir, VA				x
Legend				
x	The site where the sources of the information were obtained and the associated audit objectives.			

Source: DLA OIG Developed

EAGLE SYSTEM-SPECIFIC FINDINGS

We identified two deficiencies related to the configuration management process and programmers accessed the production environment for EAGLE.

Configuration Management Process

The EAGLE Configuration Control Board (CCB) had not been formally established and did not have consistent documentation of test cases, test results, and appropriate approval before EAGLE system changes were moved to production. The official EAGLE CCB Charter was completed and waiting to be approved by the Director, DLA Information Operations. EAGLE was implemented at the DLA field activities in 2009 and 2010 with an aggressive development and deployment schedule. Due to the aggressive development and deployment schedule, DLA Information Operations at Ogden did not have adequate resources to consistently complete the CM documentation for all changes to EAGLE. This resulted in the deferment of the customary control structure that existed for applications in a mature stage of the system development life cycle.

DODI 8500.2 required all information systems be under the control of a chartered CCB that met regularly. In addition, Chapter 4 of DLA Regulation 8250.4, "Configuration Management Appendix G – DLA Implementing Instruction for Configuration Management," required a configuration record to document all approved configuration changes to all designated configuration items.

The official EAGLE CCB Charter was completed and waiting to be approved by the Director of DLA Information Operations. DLA Information Operations at Ogden focused its priority on EAGLE implementation and deployment to the DLA Enterprise. Without an approved CCB charter in place, the authority, roles and responsibilities, and delegations were not adequately defined within the EAGLE CM process. In addition, without complete CM documentation, DLA Information Operations at Ogden could not ascertain if changes had passed through controls that were designed to protect DLA systems from unauthorized changes. Consequently, improper configuration of information system components could have negatively impacted the security posture and availability of the system.

Recommendation E1 *(Director, DLA Information Operations at Ogden)*

Coordinate with the Director of DLA Information Operations to formally establish an EAGLE CCB Charter.

Management Comments

Concurred. The EAGLE CCB Charter is completed and awaiting final approval by the Director, DLA Information Operations. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation E2 *(Director, DLA Information Operations at Ogden)*

Update the EAGLE CM policies and procedures to reflect the roles and responsibilities of the chartered EAGLE CCB.

Management Comments

Concurred. EAGLE configuration management policies and procedures are updated to include the roles and responsibilities of the chartered EAGLE CCB. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation E3 *(Director, DLA Information Operations at Ogden)*

Enforce the updated EAGLE CM policies and procedures to ensure a comprehensive CM process, which would also include the requirement for completing and retaining CM documentation.

Management Comments

Concurred. The EAGLE configuration management document was updated to include a comprehensive configuration management process to include test case development, test case results, appropriate approvals, and documentation. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Programmers Accessed the Production Environment

Two application programmers had logical access to the system that allowed them direct access to EAGLE data and programs. The logical access permitted the programmers to migrate EAGLE database and EAGLE application software code changes into the production environment. EAGLE was implemented at the DLA field activities in 2009 and 2010 with aggressive development and deployment schedules that required extraordinary efforts by DLA Information Operations at Ogden. These aggressive schedules resulted in the deferment of the customary control structure normally in place for mature applications.

NIST Special Publication 800-53 recommended that the organization employ the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) that were necessary to accomplish assigned tasks in accordance with organizational missions and business functions. DODI 8500.2 required each IAM to ensure that information ownership responsibilities were established for each DOD information system, to include accountability, access approvals, and special handling requirements. DOD Instruction 8500.2 further required the IAM to develop and implement a role-based access scheme that accounts for all privileged access and implements the principles of least privilege and separation of duties. In addition, DODI8500.2 required the IAM to maintain visibility over all privileged user assignments to ensure separation of functions.

The EAGLE development team performed code reviews and comparisons to baseline code processes that had been developed as detailed in the EAGLE Configuration Management checklist. However, the reviews were performed by the Information Technology staff that made the code changes and not an independent party. Additionally, EAGLE application programmers had logical access that permitted them direct access to EAGLE data and programs. DLA Information Operations at Ogden had a small number of qualified system development staff to adequately separate the duties between individuals changing database and program code and individuals migrating changes into the EAGLE production environment. Consequently, with application programmers having direct access to EAGLE production data and programs, DLA Information Operations at Ogden management may not have been able to detect inappropriate changes that could have negatively affected the confidentiality, integrity, and availability of the EAGLE application.

Recommendation E4 *(Director, DLA Information Operations at Ogden)*

Adequately segregate the duties between individuals that perform the EAGLE code development and code migration activities.

Management Comments

Concurred. EAGLE configuration management is researching a monitor tool to detect unauthorized changes into production. In the meantime, management will review and approve application changes and generate a checksum before publishing to production. Additionally, management will periodically review developer access to production and periodically review database audit logs. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

SUMMARY OF RECOMMENDATIONS

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
E1	Coordinate with the Director of DLA Information Operations to formally establish an EAGLE CCB Charter.	Director, DLA Information Operations at Ogden	Completed	October 2011
E2	Update the EAGLE CM policies and procedures to reflect the roles and responsibilities of the chartered EAGLE CCB.	Director, DLA Information Operations at Ogden	Completed	March 2011
E3	Enforce the updated EAGLE CM policies and procedures to ensure a comprehensive CM process, which would also include the requirement for completing and retaining CM documentation.	Director, DLA Information Operations at Ogden	Completed	March 2011
E4	Adequately segregate the duties between individuals that perform EAGLE code development and code migration activities.	Director, DLA Information Operations at Ogden	Open	August 2012

FLIS SYSTEM-SPECIFIC FINDINGS

We identified one deficiency related to the configuration management process for FLIS. FLIS mainframe system changes were inconsistently documented and tracked from initiation through migration of program code into production as part of the CM process. The CM tracking tool, Task Order Website (TOWS), did not require FLIS to be noted in the application and information field that could have been used to generate a consolidate FLIS mainframe system change report. Also, DLA Logistics Information Service did not have a procedure detailing the documentation requirements for the changes that moved into the production or staging environments and did not successfully pass through the normal CM process. Without a clearly defined CM process, management could not adequately manage system security and availability risks.

Chapter 4 of DLA Regulation 8250.4 required a configuration record documenting all approved configuration changes to all designated configuration items. Further, DODI 8500.2 required a CM process be implemented to include requirements for a verification process to provide additional assurance that the CM process was working effectively and changes outside the CM process were not permitted through technical or procedural enforcement.

DLA Logistics Information Service used two automated tools to manage and track FLIS mainframe system changes as part of the CM process. A strong configuration management process was a foundational requirement for successful vulnerability management. Configuration management comprised of a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. As a result, processes needed to be in place for controlling modification to hardware, firmware, software, and documentation in order to protect the information system against improper modifications throughout system lifecycle. DLA Logistics Information Service used TOWS to track System Change Requests (SCRs) and used the Support Magic System (recently replaced by Service Desk Express to track Problem Reports (PRs). FLIS mainframe system changes were implemented by DISA personnel once FLIS CM staff packaged the programs and notified DISA that the system changes were ready to be migrated to the production environment.

We identified the following conditions related to FLIS mainframe CM process from the system change initiation through the migration of program code into production:

a. FLIS changes to the original requirement that took place during system development were assigned alpha characters to the original SCR number; however; the documentation associated with additional changes were not separately tracked in TOWS or the Support Magic System**.**

b. FLIS SCRs were not clearly identified in TOWS. For example, 8 of 27 SCRs did not have FLIS listed within the "application & information" field in TOWS;
c. 1 of 27 SCRs was tracked outside of TOWS;
d. 1 of 45 sampled FLIS mainframe system change did not have evidence of System Change Administrator (SCA) approval before migration into production;
e. The Post Implementation Release Notice reported that the one selected SCR with four modifications were implemented on May 2, 2010; however, management represented that the notice was incorrect and the system changes were in the staging environment and were never migrated to production; and
f. The status of SCR 0EM733 with four modifications was not known. For example:
   - DLA Logistics Information Service management represented that the selected SCR 0EM733 with four modifications to the original requirements was not migrated to production. The programs resided in the FLIS staging environment since August 2010. However, the CM team represented that the code changes for SCR 0EM733 with four modifications had migrated to production, but no program library was created to run the programs. Neither management nor the CM team could provide evidence that the programs were either residing in the FLIS staging environment or in production.
   - The SCR 0EM733 with four modifications did not contain evidence that they received a successful pass confirmation from the Quality Assurance (QA) testing team and a SCA approval before the program code was moved to staging or production.

The "Application and Information" field within TOWS was not a required field; therefore, FLIS mainframe specific system changes were not identified in a system change report. For the SCR that was initiated prior to the implementation of TOWS, management did not require the staff to track in changes in TOWS. DLA Logistics Information Service did not have a procedure detailing the documentation requirements for the changes that moved into the production or staging environment but did not successfully pass through the normal CM process (i.e., QA testing, etc.) or the types of documentation required prior to changes being moved into production.

The CM group pulled the information to create the Post Implementation Release Notices from the scheduled SCRs; therefore, any changes to the status of the SCRs were not updated on the Post Implementation Release Notices. As a result, when the CM group sends the Post Implementation Release Notices to the FLIS mainframe stakeholders, they were not correct. Since DISA was responsible for migrating code from FLIS staging to the production environment, FLIS management did not have accurate information on where specific system changes or programs resided.

Without complete CM documentation, DLA Logistics Information Service management could not ascertain that changes had successfully passed through controls that were designed to protect FLIS from unauthorized changes. Consequently, improper configuration of information system components could negatively impact the security posture of the system and affect the confidentiality, integrity, and availability of the system. Without visibility on the location of the programs in the FLIS Mainframe staging environment, system changes that were no longer needed could accidentally be moved to production and adversely affect the system. With incorrect information listed in the Post Implementation Release Notices, management would not have accurate information of specific FLIS system changes that were or were not successfully implemented in production by DISA.

Recommendation F1 *(Director, DLA Information Logistics Service)*

Develop a process to ensure that SCRs and PRs are properly classified as FLIS system changes in TOWS and Service Desk Express, respectively.

Management Comments

Concurred. DLA Logistics Information Service will ensure SCRs in TOWS are properly classified as FLIS SCRs. Service Desk express currently is classifying PRs correctly. This recommendation was completed in September 2011. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation F2 *(Director, DLA Information Logistics Service)*

Re-evaluate the usefulness of the FLIS mainframe Post Implementation Release Notices. If sending out the Post Implementation Release Notices to FLIS stakeholders needs to continue, develop and implement a process to ensure accurate information is presented in the Post Implementation Release Notices and reconcile information on the notice to the data within TOWS and the Service Desk Express.

Management Comments

Concurred. DLA Logistics Information Service will reconcile the information in the post implementation release notice if changes occur. The estimated completion date is December 2011. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation F3 *(Director, DLA Information Logistics Service)*

Develop and implement a formal procedure detailing the documentation requirements for the following: (a) changes that moved to production but did not successfully progress through the normal CM process (i.e., functional testing, QA testing, etc.) and (b) the types of documentation required (i.e., SCA approval, QA results, etc.) prior to changes being moved to production.

Management Comments

Concurred. The DLA Logistics Information Service TSC Change and Configuration Management User Guide were updated to include the types of documentation required. The estimated completion date was September 2011. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation F4 *(Director, DLA Information Logistics Service)*

Coordinate with DISA to perform an inventory of the programs residing in the FLIS Mainframe staging environment and remove programs if they will not be migrated to production.

Management Comments

DLA Logistics Information Service concurred. DLA Logistics Information Service completed an inventory of the programs that resided in the FLIS Mainframe staging environment. This action was completed in October 2011. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation F5 *(Director, DLA Information Logistics Service)*

Coordinate with DISA to review and inventory the FLIS Mainframe production program libraries and remove programs that are no longer needed.

Management Comments

Concurred. As the post implementation release notice is received, the System Change Request (SCR) Administrator will conduct a reconciliation of those change requests that were implemented within TOWS. The Software Change Administrator conducted an audit of the Pre/Post release notice. The Project Manager is currently developing a Change Request (CR) to delete programs that are no longer needed. The estimated completion date is April 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

SUMMARY OF RECOMMENDATIONS

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
F1	Develop a process to ensure that SCRs and PRs are properly classified as FLIS system changes in TOWS and Service Desk Express, respectively.	Director, DLA Information Logistics Service	Completed	September 2011
F2	Re-evaluate the usefulness of the FLIS mainframe Post Implementation Release Notices. If sending out the Post Implementation Release Notices to FLIS stakeholders needs to continue, develop and implement a process to ensure accurate information presented in the Post Implementation Release Notices and reconcile information on the notice to the data within TOWS and the Service Desk Express.	Director, DLA Information Logistics Service	Completed	December 2011
F3	Develop and implement a formal procedure detailing the documentation requirements for the following: (a) changes that moved to production but did not successfully progress through the normal CM process (i.e., functional testing, QA testing, etc.) and (b) the types of documentation required (i.e., SCA approval, QA results, etc.) prior to changes being moved to production.	Director, DLA Information Logistics Service	Completed	September 2011
F4	Coordinate with DISA to perform an inventory of the programs residing in the FLIS Mainframe staging environment and remove programs if they will not be migrated to production.	Director, DLA Information Logistics Service	Completed	October 2011

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
F5	Coordinate with DISA to review and inventory the FLIS Mainframe production program libraries and remove programs that are no longer needed.	Director, DLA Information Logistics Service	Open	April 2012

DMLSS-W SYSTEM-SPECIFIC FINDINGS

We identified three deficiencies related to the configuration management process, marking and labeling of information displayed on screen, and password parameters not being in compliance with DODI 8500.2 for DMLSS-W.

Configuration Management Process

The current configuration management processes for DMLSS-W did not match the processes outlined in the CM Plan and Software Development Life Cycle (SDLC) for the Medical Information Management Division (MIMD.) In addition, we identified instances where the required appropriate approvals were bypassed and the test results could not be located for system changes that were moved to production. Both the CMP and SDLC were outdated and were being revised to fully capture the current CM process for DMLSS-W. Without a clearly defined CM process, management could not adequately identify and manage system security and the associated availability and data integrity risks.

According to DODI 8500.2, a strong configuration management process was a foundational requirement for successful vulnerability management. The Instruction also required a CM process be implemented to include requirements for a verification process to provide additional assurance that the CM process was working effectively and changes outside the CM process were technically or procedurally not permitted. In addition, Chapter 4 of DLA Regulation 8250.4 required a configuration record documenting all approved configuration changes to all designated configuration items.

Configuration management, as defined by NIST Special Publication 800-128, was comprised of a collection of activities that focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. Under the configuration management process for DMLSS-W, changes to DMLSS-W were required to go through several approval points. These approval points were called Exit Gate Reviews. Meeting these Exit Gate Reviews could have ensured the successful development, implementation, and operation of a system that required close coordination and partnership among the Program Manager, Project Integrator, and Project Team.

We identified the following deficiencies related to the design and operating effectiveness of DMLSS-W CM process:

- The current configuration management processes for DMLSS-W did not match the processes outlined in the CM Plan, dated May 11, 2010 and SDLC document for the MIMD, dated May 6, 2010. Specifically, the following processes were not addressed in the CMP or SDLC:
    - Processes for web content changes,
    - Processes for Medical Product Databank (MedPDB)-related changes, and
    - Exit Gate Reviews that could be skipped/combined for Emergency, Fixes and Minor changes.

- 6 of 45 sampled system changes did not meet all the Exit Gate Reviews required for Emergency changes,
- 5 of 45 sampled system changes did not meet all the Exit Gate Reviews required for Fix changes,
- 4 of 45 sampled system changes did not meet all the Exit Gate Reviews required for Major changes,
- 5 of 45 sampled system changes did not meet all the Exit Gate Reviews required for Minor changes, and
- 6 of 45 sampled system changes did not have test results loaded into the Visual Studio Team System (VSTS) and/or could not be located.

The MIMD was in the process of implementing and enforcing the new CM process, which also included enforcing configuration status accounting via CM documentation. Without complete CM documentation, MIMD Management could not ascertain if changes had successfully passed through controls that were designed to protect the DMLSS-W system from unauthorized changes. Consequently, improper configuration of information system components may have negatively impacted the security posture of the system and affected system confidentiality, integrity, and availability.

Recommendation G1 *(Director, Medical Information Management Division at DLA Troop Support)*

Update the Configuration Management Plan and SDLC document to reflect the current configuration management process, and implement and enforce the revised configuration management process.

Management Comments

Concurred. DLA Troop Support Medical Supply Chain Philadelphia has reviewed and updated its CM process and SLDC to fully capture the current process for the program and to comply with DODI 8500.2, and Chapter 4 of DLA Regulation 8250.4. The estimated completion date was November 2011. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Marking and Labeling

The information within each DMLSS-W application was classified as “For Official Use Only (FOUO)” and management had taken steps to update the display screens to include the proper labeling; however, 1 of 30 DMLSS-W applications did not have the required FOUO marking and labeling to alert users of the information protection requirements, due to a lack of management oversight. As a result, medical logistics information could have been mishandled that could have harmed the DLA mission through information leakage or unauthorized disclosure.

According to DOD 5200.1-R, "Information Security Program,” all personnel of the DOD were personally and individually responsible for providing proper protection to classified information under their custody and control. The marking and labeling control applied to both classified and unclassified controlled information. Marking and labeling were the principal means of informing holders of specific protection requirements for that information. The information should have been identified clearly by electronic labeling, designation, or marking. DOD 5200.1-R also required that "material other than paper documents (for example, slides, computer media, films, etc.) bear markings that alert the holder or viewer that the material contains FOUO information."

DISA hosted the DMLSS-W servers; therefore, it provided the marking and labeling on the server hardware. However, DLA Troop Support was responsible for the marking and labeling of displayed information on computer screens or websites, as well as printed material, to alert the holders or viewers that the material contained controlled unclassified information. The Defense Medical Logistics Item Identification System (DMLIIS) within DMLSS-W did not have the required FOUO marking and labeling when information displayed on screen. The FOUO marking of information on the DMLIIS application screens were inadvertently missed during the DMLSS-W web content updates. Without proper marking and labeling of DMLSS-W information, users may have mishandled information in violation of DOD policies and procedures. As a result, there was an increased risk of mishandling sensitive medical logistics information and unauthorized disclosure.

Recommendation G2 *(Director, Medical Information Management Division at DLA Troop Support)*

Enforce the marking and labeling requirements on the DMLIIS application.

Management Comments

Concurred. Both the Staging and Production environments for DMLSS-W at the DLA DOE are now compliant and all applications are properly marked with the FOUO labeling as prescribed by the DOD 5200.1-R. The recommendation was completed in June 2011. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Password Parameter

DMLSS-W used the DOD Common Access Card (CAC) and a Personal Identification Number (PIN) as the primary authentication method for the majority of the users. External users to DLA were required to use an assigned identification (ID) and password to access DMLSS-W and the MIMD had received a DOD PKI waiver from the DMLSS-W DAA for not moving all users to DOD CAC and PIN authentication method. However, the DMLSS-W password parameter did not meet the password requirements prescribed by DODI 8500.2. Without a proper password parameter, hackers may crack authorized users' passwords and perform malicious activities while emulating authorized users. Consequently, those malicious activities could significantly affect the confidentiality, integrity, and availability of DLA medical logistics data.

DODI 8500.2 required systems utilizing a logon ID as the individual identifier to have passwords that at a minimum contained: a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one each (e.g., emPagd2!). Also, at least four characters must be changed when a new password was created.

DMLSS-W current password policy exceeded the DODI 8500.2 requirements for password length by requiring that passwords be 15-32 characters long. However, the DMLSS-W password parameter only required changing one character when users created new passwords. Therefore, the DMLSS-W password parameter did not meet the minimum four characters changed requirement prescribed by DOD Instruction 8500.2. Since DMLSS-W password length exceeded DODI 8500.2 requirements, MIMD management believed that it was sufficient to mitigate the requirement of four characters changed for a new password. Weak passwords could easily be cracked by unauthorized individuals to gain access to DLA sensitive information that could put DLA mission and war fighters' safety at risk. As a result, the DAA did not have a complete view of the security posture of DMLSS-W to make an informed authorization to operate decision.

Recommendation G3 *(Director, Medical Information Management Division at DLA Troop Support)*

Update the DMLSS-W password parameter to enforce users changing at least four characters when creating a new password as required by DODI8500.2.

Management Comments

Partially Concurred. A POA&M will be submitted to ask for a waiver based on the current password policy of 15 Characters (Uppercase/Lowercase/Number/Special Character) in place at this time as a mitigating factor that increasing security and going beyond the DOD password length requirements. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive. The Medical Information Management Division should obtain a waiver if it had made an assessment that the 15 Characters password policy would mitigate the security risks addressed by not complying with DODI 8500.2 requirements.

SUMMARY OF RECOMMENDATIONS

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
G1	Update the Configuration Management Plan and SDLC document to reflect the current configuration management process, and implement and enforce the revised configuration management process.	Director, Medical Information Management Division at DLA Troop Support	Completed	November 2011
G2	Enforce the marking and labeling requirements on the DMLIIS application.	Director, Medical Information Management Division at DLA Troop Support	Completed	June 2011
G3	Update the DMLSS-W password parameter to enforce users changing at least four characters when creating a new password as required by DODI8500.2.	Director, Medical Information Management Division at DLA Troop Support	Completed	November 2011

Appendix H

DSS SYSTEM-SPECIFIC FINDINGS

We identified one deficiency related to the configuration management process for DSS. The DSS IAM or designee was not listed as a member in the DSS CCB Charter. In addition, the audit team identified instances of CM documentation stored in InfoMan that did not accurately reflect the approval of the change, type of change, or the status of test results. Consequently, management could not adequately monitor confidentiality, integrity and availability of DSS data and programs.

DODI 8500.2 required all information system be under the control of a chartered CCB. DLA Regulation 8250.4 states that the CCB should have representatives from supporting organization and the Information Assurance personnel. In addition, Chapter 4 of DLA Regulation 8250.4 required a configuration record documenting all approved configuration changes to all designated configuration items. Configuration management was comprised of a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. DLA Information Operations at New Cumberland utilized InfoMan to record and report the status of requirements and changes to DSS. The Software Configuration Management Plan for DSS required InfoMan records be updated throughout the lifecycle baseline activities. In addition, the Configuration Management Group within DLA Information Operations at New Cumberland was required to conduct periodic audits of InfoMan records to ensure compliance with the Software Configuration Management Plan for DSS.

We identified the following conditions related to the CM process for DSS:

- DSS IAM or designee was not listed as a member in the DSS CCB Charter,
- 1 of 43 DSS changes did not have the proper CM documentation to evidence that the change was approved by the Configuration Management Working Group,
- 1 of 43 DSS changes did not have the proper CM documentation to evidence the type of change, and
- 1 of 43 DSS changes did not have the proper CM documentation to evidence the final status of test results.

The formal members of the DSS CCB charters were at the senior executive level. Personnel from the IA Division had been serving in the advisory capacity to the CCB; however, the IAM, or designee, was never formally designated as an Advisory Member in the CCB Charter. In addition, the lack of proper CM documentation was due to a management oversight. Without formal designation of the IAM in the DSS CCB Charter, changes to DSS might bypass the IA review and have potentially introduced security vulnerabilities into the system. Also, without proper CM documentation, management could not have ensured that DSS changes had gone through the necessary security reviews and approvals prior to implementation in the production environment. As a result, DLA Information Operations at New Cumberland could not ensure a strong security posture to protect DSS programs and data.

Recommendation H1 *(Director, DLA Information Operations at New Cumberland)*

Update the DSS CCB Charter to designate at a minimum the IAM as an advisory member, and enforce the requirement of periodic audit of InfoMan records to ensure compliance with the Software Configuration Management Plan for DSS.

Management Comments

Concurred. DLA Information Operations at New Cumberland will revise the DSS CCB Charter to include the IAM as an advisory member and will begin periodic audits of InfoMan records to ensure compliance with the Software Configuration Management Plan for DSS. The estimated completion date is January 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

SUMMARY OF RECOMMENDATION

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
H1	Update the DSS CCB Charter to designate at a minimum the IAM as an advisory member, and enforce the requirement of periodic audit of InfoMan records to ensure compliance with the Software Configuration Management Plan for DSS.	Director, DLA Information Operations at New Cumberland	Open	January 2012

EBS SYSTEM-SPECIFIC FINDINGS

We identified two deficiencies related to the configuration management process and marking and labeling of information displayed on screen for EBS.

Configuration Management Process

A CM process was implemented for both of the Sustainment Groups and the Build Teams for EBS changes. However, we identified inconsistent documentation of tests performed on EBS changes prior to moving them into the EBS production environment. The inconsistency was caused by CM procedural documents not being formally implemented or enforced across all offices responsible for the EBS CM process. Without consistent application of standard operating procedures across all offices that performed EBS system changes, management could not adequately manage the integrity and confidentiality of EBS data.

DODI 8500.2 required a CM process be implemented to include requirements for a verification process to provide additional assurance that the CM process was working effectively and changes outside the CM process were technically or procedurally not permitted. In addition, Chapter 4 of DLA Regulation 8250.4 required a configuration record documenting all approved configuration changes to all designated configuration items.

The EBS CM process was distributed between the Build Teams and the Sustainment Groups. The Build Teams mainly focused on development of new system requirements while the Sustainment Groups focused on system management and maintenance of the system baseline. EBS was under the control of a chartered CCB and a formal CM Plan. The EBS CM Plan was supplemented by various standardized operating procedures developed for the EBS Build Teams and Sustainment Groups.

We selected a sample of 45 EBS changes and verified that each EBS change went through six control points (i.e., Team Lead approval for work to begin, Team Lead approval for system test or staging test, ready for production approval, approved for production, migration approval (unless the change was part of the Project Development Plan release), and executed production migration) before a change was implemented into the production environment. However, we identified 7 of 45 sampled EBS changes that did not contain test results to evidence that those changes were successfully tested prior to moving into the EBS production environment.

EBS Sustainment at Columbus had developed procedural documents; however, they were not formally implemented or enforced across the EBS Sustainment field offices. In addition, the standardized operating procedures for the EBS Build Teams were not consistently enforced.

Without complete CM documentation, management could not ascertain if EBS changes had successfully passed through controls that were designed to protect DLA system from unauthorized changes. Consequently, improper configuration of information system components may negatively affect the security posture and the confidentiality, integrity, availability of the system.

Recommendation I1 *(Director, DLA Information Operations)*

Review, update, implement, and enforce the procedural documents to standardize the EBS CM process across the EBS Sustainment Groups and Build Teams.

Management Comments

Concurred. DLA Information Operations at Columbus Sustainment will address this item during the EBS Production DIACAP reaccreditation process. The estimated completion date is August 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Marking and Labeling

EBS did not bear special marking or labeling on the screens or print outs and DLA Information Operations personnel could not provide documentation in support of management's decision on not having special marking and labeling on EBS screens and printouts. As a core financial management system, EBS processed many types of sensitive information such as requisition orders, payments related to procurements and inventory information related to DOD logistical support that could pose significant harm to the DLA mission if information contained in EBS was mishandled.

According to the DOD 5200.1-R, "Information Security Program," all personnel of the DOD were personally and individually responsible for providing proper protection to classified information under their custody and control. The marking and labeling control applies to both classified and unclassified controlled information. Marking and labeling were the principal means of informing holders of specific protection requirements for that information. The information should be identified clearly by electronic labeling, designation, or marking. Also, DODI 8500.2 required information and DOD information systems that store, process, transit, or display data in any form or format that was not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents, such as DOD 5200.1-R.

In 2010, DLA Information Operations conducted a data call for the review of controlled unclassified information on selective DLA systems. In response to the data call, DLA Information Operations at Columbus personnel performed an assessment on two applications within EBS, the DLA Pre-Award Contracting System (DPACS) and the DLA Internet Bid Board System (DIBBS) and determined that neither DPACS nor DIBBS required special marking and labeling. However, DLA Information Operations personnel could not provide documentation in support of management's decision on not having special marking and labeling for EBS screens and printouts needed to alert viewers of the special protection required for the displayed controlled unclassified information.

The EBS data owners made a determination that displayed and printed EBS data did not need to bear special marking or labeling. The determination was made four years ago and the data owners' decision was not documented. Without proper marking and labeling of EBS information, users may mishandle information in violation of DOD policy and procedures. As a result, sensitive procurement and logistics information and PII may be inappropriately disclosed to the public that could harm the DLA mission.

Recommendation I2 *(Director, DLA Information Operations)*

Coordinate with EBS data owners and assess the types of information within EBS to determine the marking and labeling requirements for EBS display screens and printouts that contain controlled unclassified information.

Management Comments

Concurred. DLA Information Operations at New Cumberland Sustainment will address this item during the EBS Production DIACAP reaccreditation process. The estimated completion date is August 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation I3 *(Director, DLA Information Operations)*

Document the assessment results on the types of information within each EBS application that may or may not require special marking and labeling.

Management Comments

Concurred. DLA Information Operations at New Cumberland Sustainment will address this item during the EBS Production DIACAP reaccreditation process. The estimated completion date is August 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

Management comments were responsive.

Recommendation I4 *(Director, DLA Information Operations)*

Implement the applicable marking and labeling requirements for the appropriate EBS display screens and printouts in accordance with applicable DOD policies.

Management Comments

Concurred. DLA Information Operations at New Cumberland Sustainment will address this item during the EBS Production DIACAP reaccreditation process. The estimated completion date is August 2012. Verbatim management comments can be found in Appendix J.

DLA OIG Response

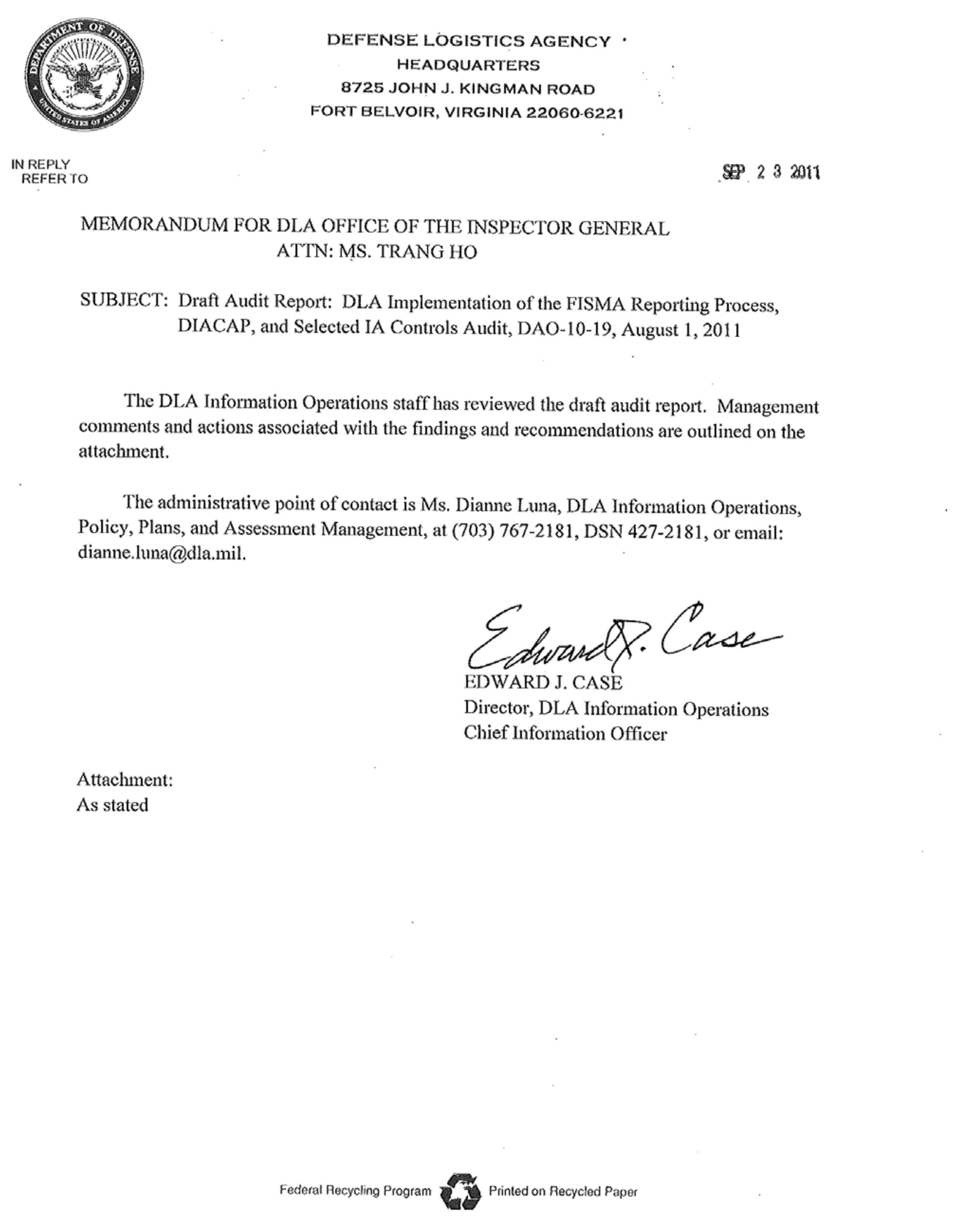
Management comments were responsive.

SUMMARY OF RECOMMENDATIONS

	Recommendation	Addressee	Status of Corrective Action	Estimated Completion Date
I1	Review, update, implement, and enforce the procedural documents to standardize the EBS CM process across the EBS Sustainment Groups and Build Teams.	Director, DLA Information Operations	Open	August 2012
I2	Coordinate with EBS data owners and assess the types of information within EBS to determine the marking and labeling requirements for EBS display screens and printouts that contain controlled unclassified information.	Director, DLA Information Operations	Open	August 2012
I3	Document the assessment results on the types of information within each EBS application that may or may not require special marking and labeling.	Director, DLA Information Operations	Open	August 2012
I4	Implement the applicable marking and labeling requirements for the appropriate EBS display screens and printouts in accordance with applicable DOD policies.	Director, DLA Information Operations	Open	August 2012

MANAGEMENT COMMENTS

Management also provided general comments on (1) auditors' testing approaches to meet the audit objectives, (2) DLA's implementation of the "trusted but verify" relationship outlined in the DLA DIACAP implementation Guide, (3) the correct terminology for the IA certification reviews of DIACAP packages performed by DLA Information Operations, Information Assurance, and (4) auditors' conclusion related to DLA generally did not implement the DIACAP in accordance with DODI 8510.01. We had analyzed management's general comments and addressed them in the report as appropriated. Verbatim management general comments can be found below.



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

IN REPLY
REFER TO

SEP 2 3 2011

MEMORANDUM FOR DLA OFFICE OF THE INSPECTOR GENERAL
ATTN: MS. TRANG HO

SUBJECT: Draft Audit Report: DLA Implementation of the FISMA Reporting Process, DIACAP, and Selected IA Controls Audit, DAO-10-19, August 1, 2011

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 Ms. Dianne Luna, DLA Information Operations, Policy, Plans, and Assessment Management, at (703) 767-2181, DSN 427-2181, or email: dianne.luna@dla.mil.

Edward J. Case

EDWARD J. CASE
Director, DLA Information Operations
Chief Information Officer

Attachment:
As stated

Federal Recycling Program Printed on Recycled Paper

Recommendation 1. Develop policy and procedure for retention of supporting data used for FISMA reporting.

DLA Comments. **Partially concur**. DLA HQ IT Continuity of Operations Plan (COOP) Team developed a collaboration room for retention of supporting data used for FISMA reporting. It can be found at, https://eworkplace.dla.mil/Pages/Default.aspx. This collaboration site is a joint repository for J6 FISMA report data. Completed November 2010

Recommendation 2. Update and enforce the validation and verification process to assess and document the design and operating effectiveness of all Information Assurance (IA) controls for DLA systems.

DLA Comments. **Nonconcur**. The validation process is clearly defined in Department of Defense (DoD) Instruction (DODI) 8510.01 and the DLA DIACAP Implementation Guide, plus the DIACAP KS Web Portal goes into specific detail with regards to the assessments steps, required artifacts, expect results, etc. for every IA control to be assessed. The DLA implementation of DIACAP assigns the responsibility for ensuring that these validation activities are carried out, validated, and confirmed with the respective J6 Site Director or Program Manager Officer (PMO) director (Program Executive Office (PEO), Program Manager (PM), etc.). This is the specific reason J6 Site Directors were appointed as certification and accreditation (CA) Representatives as part of the DLA DIACAP implementation. DLA Information Operations, Information Assurance (J61) performs the IA certification review (e.g., verification) that all assigned IA controls have had their applicability, implementation, and compliance status validated, and through that IA certification review, in conjunction with the CA Representative's System/Program Manager (SM/PM) and IA Managers (IAM) validation an accreditation recommendation for the Designated Approving Authority (DAA) is derived.

Recommendation 3. Conduct an evaluation of all applicable IA controls and assign baseline IA controls for each DLA system in Enterprise Mission Assurance Support System (eMASS) to include an accurate identification of inherited, shared, and DLA-owned IA controls.

DLA Comments. **Partially concur.** The recommendation is not totally clear in terms of what the auditors are attempting to identify as a deficiency, or what the recommendation requires of J6 that isn't already part of the DLA DIACAP implementation. As a functional tenant of the process, an evaluation of applicable IA controls is the basis from which the IA posture of information systems undergoing certification and accreditation (C&A) is determined. Inexplicably, the process in and of itself cannot be executed with conducting an evaluation of all applicable IA controls assigned to a given information system to include the identification of inherited and shared IA controls. This is a given requirement in order complete the validation of all assigned IA controls and is clearly documented in the DLA DIACAP Implementation Guide as such. Lastly, the facilitation of the process via eMASS cannot be processed without the assignment of baseline IA controls, which are derived from the information systems Mission Assurance Category (MAC) and confidentiality level that are entered into eMASS upon registration of the information system.

Recommendation 4. Enforce the requirement that a program or system manager be designated for each DLA system and who will perform the functions in accordance with DODI 8510-01 and the DLA DIACAP Implementation Guide.

DLA Comments. **Partially concur.** Designation of either a SM or PM is a requirement per DODI 8510.01 and the DLA DIACAP Implementation Guide. It applies to all information systems. Additionally no DLA DIACAP package has been approved without a SM/PM assigned in eMASS. However, it is incumbent on the system owner (e.g., J6 Field Site Director) to ensure that the assignment of a responsible SM/PM is done in a manner in which the individual assigned is responsible for all the inherent responsibilities of such an assignment. J61 has reinforced this requirement in the updated DLA Instruction 6401, "IA Management Controls." ECD: September 2011. This update instruction will be submitted to DLA Information Operations, Policy, Plans, and Assessment Management (J65) for formal coordination and approval.

Recommendation 5. Coordinate with the Director of DLA or obtain the delegation of authority to update the DLA Enterprise Service Support Document (ESSD) and SLAs with Defense Information Systems Agency (DISA) to explicitly define the expected level of services and IA roles and responsibilities.

DLA Comments. **Concur.** DLA Enterprise Solution (J64) and DISA have a team reviewing the DLA ESSD to ensure: An enterprise approach is implemented, clear IA boundaries are identified and the service levels are clearly defined. ECD: The milestone dates are being finalized and will be published.

Recommendation 6. Coordinate with DISA to explicitly define listings of system-specific inherited, shared, and customer owned IA controls for all DISA hosted DLA systems.

DLA Comments. Concur. J64 and DISA have a team reviewing the DLA ESSD to ensure: An enterprise approach is implemented, clear Information Assurance boundaries are identified and the service levels are clearly defined. ECD: The milestone dates are being finalized and will be published.

Recommendation 7. Communicate guidance to the Director of DLA Information Operations at Ogden on the minimum information that must be reviewed and communicated back to DLA Information Operations to update the SLAs with DISA on an annual basis.

DLA Comments. Concur. DLA and DISA established a team to work with all DLA stakeholders to ensure communication is clear. SLAs are part of the ESSD revision and DLA Information Operations at Ogden are included as stakeholders. ECD: The milestone dates are being finalized and will be published.

Recommendation 8. Update the DLA DIACAP Implementation Guide to provide detail instructions on the standard format and appropriate artifacts in support of the residual risk analysis for IT security weaknesses reported on the POA&Ms.

DLA Comments. Nonconcur. The DLA DIACAP Implementation Guide clearly establishes the requirement for the documenting all identified IA control related system weaknesses as a part of the validation activities associated with certifying and accrediting all DLA information systems in accordance with DODI 8510.01. In addition, J6 has documented requirements and guidance in the “Preparation of IT security POA&Ms” policy memorandum. This policy memorandum was signed by the J6 Director in March 2009 and has been in effect since that date. This policy memorandum enumerates the POA&M requirement, as well as describes in detail the required format and intended information for each section of the POA&M.

Recommendation 9. Implement an enterprise procedure for disseminating, tracking, and managing DLA IT security weaknesses identified as the result of internal or external assessments or audits (i.e., IA security assessments during the C&A process, annual system security review, DLA OIG audits, GAO audit, and DOD IG audits).

DLA Comments. **Nonconcur.** The DLA DIACAP implementation is the procedure for disseminating, tracking, and managing DLA IT security weaknesses identified as the result of internal or external assessments or audits, when it is applicable C&A (e.g., an existing accreditation, an information system undergoing C&A, etc.), or IA controls specifically. This is also supplemented by the “Preparation of IT Security POA&Ms” policy memorandum. The distinction of whether or not all weaknesses identified during internal or external audits should be documented in the IT Security POA&M utilized during the C&A process cannot be ignored because there are different types of POA&Ms (e.g., IAVM POA&M) that are managed and tracked differently dependent upon what process or program that particular POA&M supports.

Recommendation 10. Develop and implement a process for validating evidence that corrective actions for security weaknesses have been fully resolved and the corrective actions have been tested for the deficiencies before marking POA&Ms as completed.

DLA Comments. **Nonconcur.** J61 has established a POA&M Tracking Program, in which every POA&M item for all accredited information systems are tracked via a monthly meeting to discuss the current status, to include milestone completion date changes and mitigation/corrective action implementation progress. This program coincides with the inherent responsibilities of the system/program manager and IAMs for all accredited information systems, which is to maintain the accredited IA posture and to ensure all documented POA&M items, are tracked and managed through to resolution. The DIACAP is the process by which this is validated, maintained, and verified on a continuous basis.

Recommendation 11. Coordinate with DISA to obtain validation test results and applicable supporting artifacts for inherited IA controls.

DLA Comments. **Concur.**

- J61 has previously reached an agreement with the DISA Computing Services

Division (CSD) on the transparency of IA control reviews performed in the validation of inherited IA controls. This agreement dealt with the 32 IA controls identified in the DISA CSD Catalogue of Services.

- However, that agreement has not been followed up on, and the documented evidence supporting the compliance status for the 32 IA controls inherited by default from DISA CSD need to be obtained. J61 will reengage DISA CSD IA points of contact concerning this matter by September 8, 2011, and will update the OIG once the information is obtained.

- It should also be noted that IA controls beyond the 32 IA controls identified in the DISA CSD Catalogue of Services, are the responsibility of the inheriting information system owner (e.g., J6 Site Director, PEO, SM/PM). The responsible individuals must ensure the necessary collaboration with DISA and document any agreements reached and obtain the supporting evidence required to support the IA control's compliance status.

Recommendation 12. Designate viable alternate system recovery site(s) for EAGLE, DMLSS-W update COOP documentation, and perform COOP testing. In the interim:

- Create a POA&M in order to establish and implement mitigating controls until designated alternate system recovery site(s) are established, such as selecting temporary system recovery site(s);
- Provide an estimated timeline to have designated alternate system recovery site(s) in place and operational; and
- Update COOP documentation for each system to reflect the designated alternate system recovery site(s), the correct MAC level, and perform COOP testing using the recovery site(s).

DLA Comments. **Concur.**

- Sites were advised that Business Impact Analysis (BIA) be created for EAGLES and DMLSS-W to present to Director. IT Sites will create POA&M to mitigated contingency controls until the designated alternate recovery location is operational by during Memorandum of Agreement (MOA) with others DLA sites.
- The estimated timeline to have a designated alternate system recovery site in place and operational for the DLA Ogden Enclave which includes Eagle and DMLSS-W applications by March 31, 2012.
- DLA HQ IT COOP Team will provide the sites with the applications that will be hosted at the alternate location. IT Sites Program Managers will update sites developed BIA for approval by J6 Director for COOP capabilities. The COOP documentation will be update to include the correct MAC level for the applications. The DLA HQ COOP Team will coordinate with the IT sites and the alternate location to schedule functional exercises after the operational date of March 31, 2012.

Recommendation 13. Implement activities to improve the viability of EBS alternate system recovery site. For example,

- Update the C&A documentation in eMASS to accurately reflect the designation of the DISA, Mechanicsburg, PA, facility as the alternate recovery site;

- Complete the coordination with the key stakeholders and user representatives to develop a BIA document and to create and/or update a business continuity planning document and the IT continuity plan; and
- Ensure the completion of an upgrade to the backup and recovery infrastructure at DISA facility in Mechanicsburg, PA, in order to meet future requirements.

DLA Comments. Partially concur.

- **Concur.** J61 and J64 working with the Information Assurance Officer (IAO) or subject matter expert (SME) to make the corrections in eMASS about COAS-1 Controls because EBS does have an alternate site. EBS in eMASS is being updated.
- **Concur**. EBS IT COOP has been updated. It includes business continuity planning as of April 4, 2011 and received all necessary signatures on September 8, 2011.
- **Nonconcur**. DLA does not own the building; therefore, infrastructure at the DISA facility in Mechanicsburg, PA, is a DISA responsibility. DLA will update the Enterprise Telecommunications Network (ETN) for recovery.

Recommendation 14. Establish, at a minimum, a list of supporting documentation or artifacts that are required as part of the DLA system certification process (i.e., system-level or IA control-specific artifact) to meet OMB Circular A-130 requirement for a system Security Plan (SSP).

DLA Comments. Nonconcur.

- This nonconcurrence is in part due to the fact that the DODI 8510.01 is the DOD's guidance for adherence to the requirement documented in the Office of Management and Budget (OMB) Circular A-130, Appendix III. The DIACAP establishes a process, by which all of the requirements defined in OMB A-130, Appendix III are captured within the DIACAP package, which consists of a System Identification Profile, DIACAP Implementation Plan, DIACAP Scorecard, POA&M, and associated artifacts. OMB A-130, Appendix III is referenced in DODI 8510.01 in Enclosure 1, (S), and page 26.

- As the J6 Directorate responsible for the oversight and management of the DLA C&A process, J61 has conferred with the J6 Director/DAA on the DLA CA's interpretation of DODI 8500.2 IA control DCSD 1-1. The interpretation is that the compilation of a DIACAP package's Systems Identification Profile, the DIACAP Implementation Plan supported by the IA control test results data. The data is archived in DLA's instance of the eMASS, and the resulting DIACAP Scorecard contains the same information as a DIACAP Technical Advisory Group (TAG) prescribed SSP, and; therefore, alleviates the requirement for the development of a separate and distinct SSP.

- J61 has forwarded this interpretation on to the DIACAP TAG Chairperson for either the Office of the OSD/NII's concurrence or nonconcurrence. OSD/NII (i.e., the DIACAP TAG Chairperson) has responded and provided concurrence with J6's interpretation of this requirement and the J6 Director will sign a J6 Decision Memorandum making this the Agency's official interpretation of DCSD 1-1 (attached to this response in General Comments).

Recommendation 15. Standardize the required artifacts in support of the C&A process, such as establishing standard template(s) to ensure the consistency of information reported to the DAA.

DLA Comments. Partially concur.

- The establishment of a minimum set of required artifacts that must accompany every DIACAP package submitted; however, this mandate does not alleviate the requirement for all IA controls requiring substantiating artifacts and that these artifacts be produced and available upon request by the CA or the DAA. This mandate will seek to standard DIACAP package submissions to ensure a baseline of consistency across the enterprise. The updated version of the DLA DIACAP Implementation Guide is scheduled to be staffed and coordinated within J6 no later than September 30, 2011.

- With regards to the establishment of standard templates for required artifacts, DOD in many instances has established standard templates for a large number of artifacts. The standardization of artifacts should, however, be reserved on a case-by-case basis because of the overhead required to maintain and manage standard templates, along with taking account of all the differing operating environments across the enterprise, certain template artifacts may not be sufficient nor the most efficient means for documenting required evidence IA control compliance. Additionally, J61 would request that DLA OIG be more specific with regards to what specific artifacts they are recommending standard templates for in the final report associated with this audit.

Recommendation 16. Develop and enforce an Agency-level policy and procedure for the account management process that include the granting, modifying, terminating, and recertifying of user accounts.

DLA Comments. Concur.

- The Hire to Retire (H2R) Process Cycle Memorandums (PCM) describes the DLA process for employee transfers and/or terminations. The EAGLE Roles Guide describes EAGLE access, roles, and privileges. The DLA Finance Payroll Centers of Excellence (CoE) are responsible to add, transfer, separate and archive Government employee records in EAGLE.

- Because of the restrictions and requirements already mandated within DOD for access to local enclaves, an EAGLE user would first have to be authorized and granted access at the enclave level; a user could not access EAGLE without prior enclave access which is controlled by site administration at each enclave. The steps mentioned above are on top of the access rules mandated for DOD systems. Even though a user may still be listed with authorized access into EAGLE, the user would not be able to access through their enclave; therefore, there would be no vulnerability. All EAGLE users have to login into their local enclave via CAC before they can access EAGLE. These requirements need to be met at each local Enclave and then further restricted and verified at the COEs.

Recommendation 17. Develop and enforce the following:

- Policies and procedures for proper retention and completion of the system access authorization request that contain specific instructions, including required blocks of the form/data fields that must be completed for each type of system access request (i.e., authorized, privilege, modification to current role, recertification, termination, etc.) and

- A mechanism to monitor compliance with the agency-wide account management process.

DLA Comment. Concur. EAGLE is planning to move to AMPS to process, approve, and maintain EAGLE DD Form 2875 which will ensure standard policies and procedures are in place. The EAGLE team has been working with the AMPS team and DLA Finance HQ J892**.**

Recommendation 18. Enforce the requirement that all EBS users only are granted access or current roles be modified through AMPS and complete the AMPS revalidation of users converted from the legacy account provisioning application.

DLA Comments. Concur. AMPS can produce a list of known users and roles for EBS, but the administrative burden on the EBS administrators to do reconciliation would be huge. This would not be necessary once all of EBS is direct provisioned.

Recommendation 19. Develop a process to periodically reconcile user accounts and roles within AMPS to user accounts and roles within EBS. Additionally, the process should include a reconciliation of active roles within AMPS against active roles within EBS.

DLA Comments. Concur. Policy ECD: June 2012

Recommendation 20. Enforce DLA policy for recertifying DMLSS-W user's accounts and roles on an annual basis.

DLA Comments. Concur. DMLSS-W program is in the process of its IA annual review. Documentation specific to access (Web Access Management SOP) being update to address account recertification, as well as revalidation on an annual basis, and the IAO is being designated as the responsible for reviewing and identifying accounts. ECD: November 30, 2011

Recommendation 21. Complete the current efforts to design and document DSS user profiles that are role-based and follow the principle of least privilege. After which, management should develop a process to implement DLA policy for granting, modifying, disabling, terminating and recertifying user accounts for all DSS users.

DLA Comments. Concur. We appreciate the recognition of the audit that fixes were underway for this finding prior to the visit, and that we are on the right track. DLA Information Operations at New Cumberland has been facilitating an effort, along with other key stakeholders and users, to implement role-based access and profile realignment. The recommendation falls in line with the stated directions of the effort and, as such, work will be nearing completion this year and early next on several threads of this rather large, complex effort. DSS user profiles have been re-designed and are now in testing phase with documentation of each being finalized. DLA Distribution and DLA Information Operations at New

Cumberland continue to test the DLA Distribution approved DSS RBAC structure with DISA DECC-Mechanicsburg. With the rollout of RBAC, DSS centralized account administration will begin and will comply with the intent of this audit and DLA directives to grant, modify, disable, and terminate accounts. To improve further, we are working the DLA AMPS team for an automated revalidation tool. ECD: DSS RBAC is scheduled to be implemented at DECC-M by the end of 2011, and at DECC-Ogden by February 2012.

Recommendation 22. Centralize the administration of DSS user provisioning, modification, disabling, and termination to enhance management oversight of user accounts by the IAO.

DLA Comments. Concur. DLA Information Operations at New Cumberland agrees with the comment and will cut over to a centralized DSS account administration methodology concurrent with the west RACF cutover. As the groundwork is in place with DSS accounts at DECC-M, final action entails re-routing DD Form 2875 requests for DSS DECC-O through the same process.

Recommendation 23. Centralize the administration of EAGLE user provisioning, modification, disabling, and termination to enhance management oversight of user accounts by the IAO.

DLA Comments. Nonconcur. This recommendation is outside the scope of the DLA J6 because the data is not owned by DLA Information Operations. DLA Finance Payroll Centers of Excellence (COE) are responsible for provisioning, modification, disabling, and archiving of EAGLE user accounts and are the EAGLE data owners. Subsequent to this finding, the COE's and J8 met and developed a standard process for handling and administering EAGLE user accounts.

Recommendation 24. Develop a DLA policy and procedure for assessing and establishing the minimum background investigation and clearance requirements for all users internal to DLA accessing DLA information systems.

DLA Comments. Nonconcur. DLA follows the guidance outlined in DODI 8500.02 which prescribes procedures for investigative levels of 1, 2, and 3. This instruction also prescribes procedures for applying integrated, layered protection of the DOD information systems and networks. The DLA Security Representative Handbook dated October 2008, provides additional DLA guidance to the security workforce.

Recommendation 25. Incorporate the minimum personnel security requirements into a DLA access control policy and system level procedures to ensure an adequate verification of personnel security control is being performed prior to granting access to DLA information systems and as a part of the user account recertification process.

DLA Comments. Concur. DMLSS-W does not maintain security documentation with reference to clearances. This functionality is done by Base/Security Compound Office personnel. It is up to the business units to verify need to know access prior to submitting request. External users are not verified by DLA Troop Support RSA Access Manager Administrators. Instead their information is verified by each applications business unit personnel. ECD: November 30, 2011

Recommendation 26. Develop a process to retain evidence for verification of personnel security requirements.

DLA Comments. Concur.

Recommendation 27. Develop a process to ensure that all users internal to DLA complete IA awareness training prior to access being granted to DLA systems, and enforce IA awareness refresher training for users internal to DLA as a condition of continued access to DLA information systems.

DLA Comments. Nonconcur.

- J6 has processes in place for requiring both periodic and initial user IA Awareness training. This is executed at the J6 Field Site/PMO and business area level. The IA training completion is verified prior to granting access to any DLA Network through the System Authorization Access Request process via a DD Form 2875. Prior to gaining access to a DLA application, users are required have a DLA Local Area Network (LAN) account, and to complete a DD Form 2875 for each application; box 10 of the DD Form 2875 has a field for the entry of the most current IA Awareness training completion date. For new users requesting access to a DLA network and/or application and they have not completed the IA Awareness training, DLA policy allows 30 days to complete the training.

- The IA awareness refresher training is tracked through DLA's Learning Management System (LMS) and verified through the Account Management and Provisioning System (AMPS). As part of the ongoing DLA LAN account annual validation, AMPS checks to ensure that the user has completed the IA Awareness training within the last year. In addition, LMS and Skillport's database both alert users of the need to retake the training annually. Additionally, on a monthly basis, J61 receives a delinquency report for those users who have not completed the training within the last year. This report is submitted to J64 for distribution and tasking to the J6 Site Directors, PMOs and Business Areas for action. If the user does not complete the training in a timely fashion their LAN account is disabled, which will also disable their access to DLA applications.

Recommendation 28. Develop a policy and procedure requiring a definition of what constitutes an internal and external user to DLA for each system. In addition, document in the system access policy for each DLA system the IA awareness training and security clearance verification requirements for the defined internal and external users.

DLA Comments. Concur.

Recommendation 29. Coordinate with the subject matter experts to establish listings of available user functions/roles for BSM-E and PORTS.

DLA Comments. Concur. DLA Information Operations at Fort Belvoir is continuing to work with DLA Energy to resolve the issues identified. The Energy Convergence (EC) Program Office has been made aware of these findings and DLA Information Operations at Fort Belvoir will work with them to ensure that the recommendations are addressed in the EC.

Recommendation 30. Coordinate with the subject matter experts to establish listings of the permissible/not-permissible combination of functions/ roles for BSM-E, PORTS, and DFAMS.

DLA Comments. Concur. DLA Information Operations at Fort Belvoir is continuing to work with DLA Energy to resolve the issues identified. The EC Program Office has been made aware of these findings and DLA Information Operations at Fort Belvoir will work with them to ensure that the recommendations are addressed in the EC.

Recommendation 31. Ensure the established listings of available user functions/roles and permissible/not permissible combination of functions/roles that are critical to protecting DLA Energy systems be incorporated in the Energy Convergence system requirements and system documentation.

DLA Comments. Concur. DLA Information Operations at Fort Belvoir is continuing to work with DLA Energy to resolve the issues identified. The EC Program Office has been made aware of these findings and DLA Information Operations at Fort Belvoir will work with them to ensure that the recommendations are addressed in the EC.

Recommendation 32. Establish a formal Disaster Recovery/COOP Training Program across the DLA Enterprise for recovery team personnel.

DLA Comments. Partially concur. DLA Enterprise Disaster Recovery/COOP Training Program is in place. DLA HQ IT and HQ Business COOP Team has joined the FEMA Team to offer formal Disaster Recovery/COOP Training to site COOP coordinators and Planners. This program includes the Continuity Excellence Series (Professional Continuity Practitioner Programs).

Recommendation 33. Identify all supported systems, including RM, under the HQ ITS COOP Plan.

DLA Comments. Partially concur. The current HQITS IT COOP Plan (April 2011) includes RM under section 1.3 “Scope”**.**

Recommendation 34 (E1). Coordinate with the Director of DLA Information Operations to formally establish an EAGLE CCB Charter.

DLA Comments. Concur. The EAGLE CCB Charter is completed and awaiting final approval by the Director, DLA Information Operations.

Recommendation 35 (E2). Update the EAGLE CM policies and procedures to reflect the roles and responsibilities of the chartered EAGLE CCB.

DLA Comments. Concur. EAGLE configuration management policies and procedures are updated to reflect the roles and responsibilities of the chartered EAGLE CCB.

Recommendation 36 (E3). Enforce the updated EAGLE Configuration Management (CM) policies and procedures to ensure a comprehensive CM process, which would also include the requirement for completing and retaining CM documentation.

DLA Comments. Concur. The EAGLE CM document was updated to include a comprehensive configuration management process to include test case development, test case results, appropriate approvals, and documentation. The EAGLE PM has reviewed the new procedure with the appropriate personnel and will periodically monitor the new processes for adherence.

Recommendation 37 (E4). Adequately segregate the duties between individuals that perform EAGLE code development and code migration activities.

DLA Comments. Concur. See EAGLE Programmer Access POA&M under General comments.

Recommendation 38 (F1). Develop a process to ensure that SCRs and PRs are properly classified as FLIS system changes in Task Order Web Site (TOWS) and Service Desk Express, respectively.

DLA Comments. Concur. DLA Logistics Information Service will ensure SCRs in TOWS are properly classified as FLIS SCRs. Service Desk express currently is classifying PRs correctly. ECD: September 2011

Recommendation 39 (F2). Reevaluate the usefulness of the FLIS mainframe Post Implementation Release Notices. If sending out the Post Implementation Release Notices to FLIS stakeholders needs to continue, develop and implement a process to ensure accurate information presented in the Post Implementation Release Notices and reconcile information on the notice to the data within the TOWS and the Service Desk Express.

DLA Comments. **Concur.** DLA Logistics Information Service will reconcile the information in the post implementation release notice if changes occur. ECD: December 2011

Recommendation 40 (F3). Develop and implement a formal procedure detailing the documentation requirements for the following:

- Changes that moved to production but did not successfully progress through the normal CM process (i.e., functional testing, QA testing, etc.) and
- The types of documentation required (i.e., SCA approval, QA results, etc.) prior to

changes being moved to production.

DLA Comments.

- **Concur.** ECD: December 2011
- **Concur.** ECD: August 2011

Recommendation 41 (F4). Coordinate with DISA to perform an inventory of the programs residing in the FLIS Mainframe staging environment and remove programs if they will not be migrated to production.

DLA Comments. Concur. This finding was completed and closed on June 27, 2011.

Recommendation 42 (F5) Coordinate with DISA to review and inventory the FLIS Mainframe production program libraries and remove programs that are no longer needed.

DLA Comments. Concur. ECD: June 2012

Recommendation 43 (G1). Update the CM Plan and SDLC document to reflect the current configuration management process, and implement and enforce the revised configuration management process.

DLA Comments. Concur. DLA Troop Support Medical Supply Chain Philadelphia has reviewed and updated its CM process and SLDC to enforce and comply with and fully capture the current process for the program, meeting DODI 8500.2 and Chapter 4 of DLA Regulation 8250.4 that captures a configuration of record documenting all approved configuration changes to all designated items. ECD: November 30, 2011

Recommendation 44 (G2). Enforce the marking and labeling requirements on the DMLSS application.

DLA Comments. Concur. Both the Staging and Production environments at the DLA DOE are now compliant and all applications are properly marked with the FOUO labeling as prescribed by the DOD 5200.1-R. All delinquent applications went through the approved CM/SDLC process at DLA Troop Support and were approved and implemented. ECD: Closed. We completed the changes on/before June 13, 2011 (screen shots will be provided in with our annual eMASS package for the IA Annual Validation)

Recommendation 45 (G3). Update the DMLSS-W password parameter to enforce users changing at least four characters when creating a new password as required by DODI 8500.2.

DLA Comments. Partially concur. Please note that currently, policy is a 15 Character (Uppercase/Lowercase/Number/Special Character) is in place at this time as a mitigating factor increasing security and going beyond the DOD password length requirements. RSA Access Manager is a

Commercial-off-the-Shelf (COTS) product that is found on the current DLA IT Solutions document, as well as being Common Criteria (CC) EAL Level III Certified as of November 2009. ECD: November 30, 2011. We will be submitting a POA&M for this control. We will be asking that it be assigned to a CAT III control based on our mitigating controls in place today.

Recommendation 46 (H1). Update the DSS CCB Charter to designate at a minimum the IAM as an advisory member, and enforce the requirement of periodic audit of InfoMan records to ensure compliance with the Software Configuration Management Plan for DSS.

DLA Comments. Concur. DLA Information Operations at New Cumberland agrees with the recommendation and will revise the DSS CCB Charter to include, by name, the IAM as an advisory member. The IAM is now included in appropriate DSS meetings. HQ J64 will complete the staffing of the DSS charter and facilitate final staff action and signatures. In the interim and until the charter is signed, the IAM will be invited as a guest advisor to DSS CCB meetings. Additionally, periodic audits of InfoMan records to ensure compliance with the Software Configuration Management Plan for DSS will begin in the fourth quarter 2011. While the current DSS configuration management methodology aligns with DLA 8250.4, we are re-evaluating the methodology against DLA 8250.4 and will adjust the methodology as necessary to ensure compliance.

Recommendation 47 (I1). Review, update, implement, and enforce the procedural documents to standardize the EBS CM process across the EBS Sustainment Groups and Build Teams.

DLA Comments. Concur. DLA Information Operations at Columbus Sustainment will address this item during the EBS Production DIACAP reaccreditation process. ECD: August 2012

Recommendation 48 (I2). Coordinate with EBS data owners and assess the types of information within EBS to determine the marking and labeling requirements for EBS display screens and printouts that contain controlled unclassified information.

DLA Comments. Concur. DLA Information Operations at New Cumberland Sustainment will address this item during the EBS Production DIACAP reaccreditation process. ECD: August 2012 NOTE: J624 thinks this needs to be assigned directly to the PO/PI community for action vice J6C.

Recommendation 49 (I3). Document the assessment results on the types of information within each EBS application that may or may not require special marking and labeling.

DLA Comments. Concur. DLA Information Operations at New Cumberland Sustainment will address this item during the EBS Production DIACAP reaccreditation process. ECD: August 2012

Recommendation 50 (I4). Implement the applicable marking and labeling requirements for the appropriate EBS display screens and printouts in accordance with applicable DOD policies.

DLA Comments. Concur. DLA Information Operations at New Cumberland Sustainment will address this item during the EBS Production DIACAP reaccreditation process. ECD: August 2012

General Comments:
Comments pertaining to the Report's Introduction, Results, Recommendations and Concurrence/Nonconcurrence:

Page 2 – J61 does not agree with the second objective listed based on the approach taken during this audit. The audit primarily focused on specific information systems and the responsible personnel's application of the process (i.e., DIACAP) in certifying and accrediting the systems reviewed as evidenced by the resulted documented within the report. The audit did not focus on the process and its implementation within J6 as a primary objective.

Page 8 – J61 response to the three deficiencies identified relating to the "DLA Certification and Accreditation (C&A) Process":

Excerpt from the audit report: "The DLA DIACAP validation processes and procedures designed to reinforce the "trust but verify" relationship did not effectively detect weaknesses that existed within the C&A packages for EAGLE, FLIS, DSS, and EBS."

- This is not totally accurate, the validation activities outlined in the DLA DIACAP Implementation Guide are exact derivatives from the DODI 8510.01 and they are <u>NOT</u> designed to bolster any trust but verify relationship between the CA and the responsible SM/PM or PMO. The "trust but verify" paradigm was established through the assignment of IAM and CA Representatives for each DLA information system undergoing accreditation. This paradigm is applied to ensure the most accurate data and compliance status as it relates to the implementation and operation of IA controls is concerned, as well as providing a level of assurance that reviews and approvals have occurred through the entire scope of the management chain within DLA J6 Field Site and PMO locations.

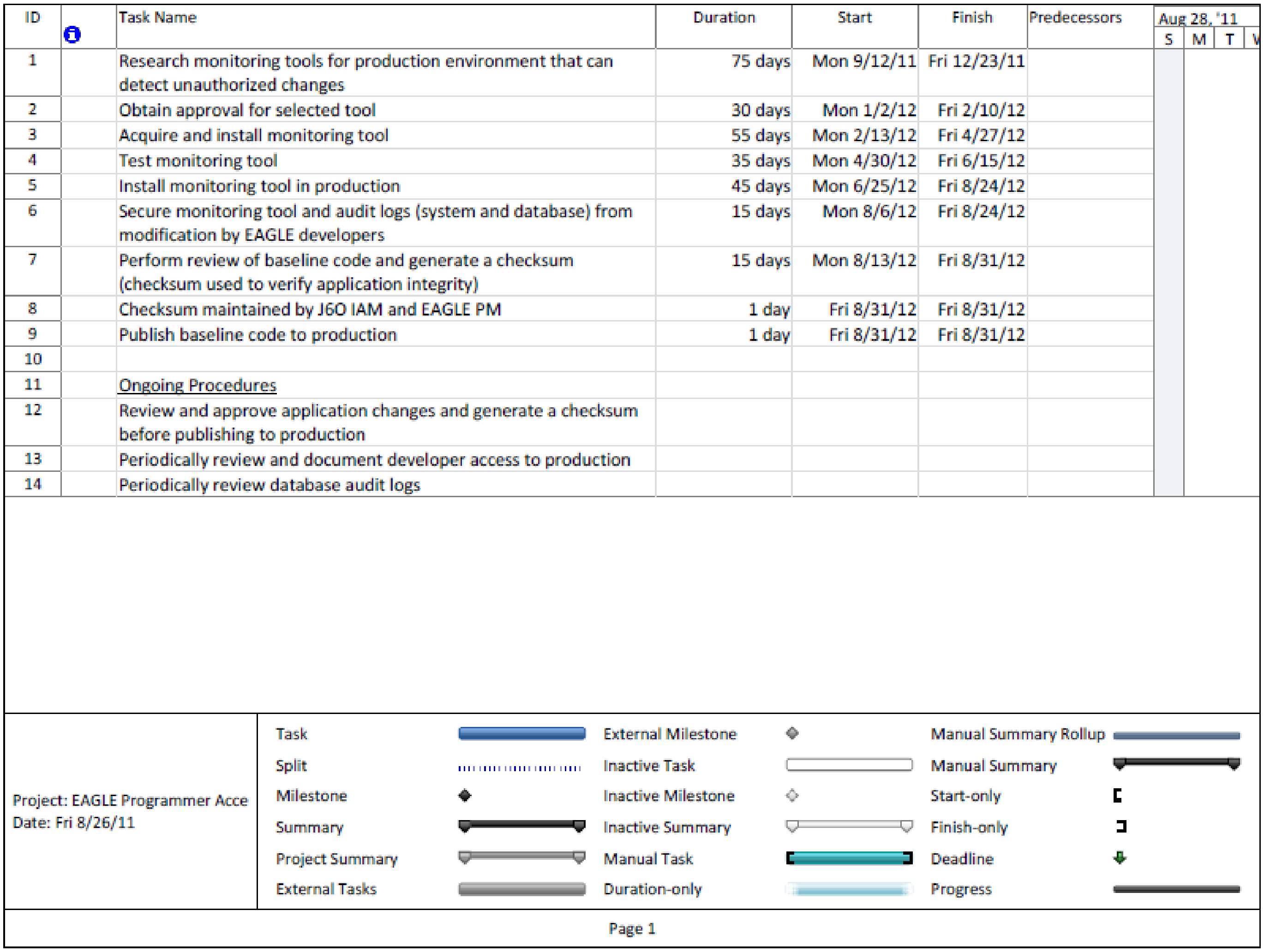
Excerpt from the audit report: "DLA Information Operations relied on the C&A verification process for a review of artifacts in eMASS before certification determination; however, there was no guidance on the types of required documentation to support security validation results that needed to be a part of the system C&A package. Consequently, DLA systems could receive an authorization to operate with severe security risks that would compromise the confidentiality, integrity and availability of DLA information systems."

- There is no such process called the "C&A Verification Process" documented in either the DLA DIACAP Implementation Guide or DODI 8510.01. J61 performs IA certification reviews of all DIACAP packages submitted to verify the proper assignment, implementation, and compliance status of all applicable IA controls. This includes a detailed review of every aspect of the required DIACAP (e.g., the System Identification Profile, DIACAP Implementation Plan, DIACAP Scorecard, and POA&M). Additionally, the eMASS facilitates the documenting of the compliance status of IA controls within the tool as well the capability to import associated artifacts and the IA certification review leverages this capability. To the contrary of what is stated above, there is specific guidance provided for the types of documentation (e.g., artifacts) required to support the validation results for every DIACAP package. This guidance is located via the DIACAP KS at https://diacap.iaportal.navy.mil/ks/. This is the official Web Portal for DOD level DIACAP policy and implementation guidance. The DIACAP KS provides DOD a single authoritative source for execution and implementation guidance to include the latest information and developments concerning the DIACAP. The DIACAP KS supports both eMASS and non-eMASS implementations of the process. The DIACAP KS includes electronic copies of department level DIACAP policy, a collection of template tools, diagrams, process maps, and documents to aid in DIACAP planning and execution. The DIACAP KS is maintained by the DIACAP TAG.

Page 22 – The draft reports makes the statement that "Accounts were created prior to documented approval for 10 of 45 EAGLE users sampled." The EAGLE Account Creation date is the date the employee's account is created in EAGLE for the purpose of creating time and attendance data to be sent to the Defense Civilian Payroll System so employees can get paid. If these accounts are not created in EAGLE, an employee would not get paid. It has no relation to the DD Form 2875 approval date for any EAGLE roles. This was reported to DLA OIG directly on April 22 via email. It was included on the J6 HQ official response to DLA OIG on document name: DIACAP-FISMA NFRs-COMMENTS J6 HQ.PDF; Pages 58 – 60. It appears that DLA OIG took no action to remove the discrepancy.

Page 35 – Conclusion (2nd paragraph, 1st sentence) "Additionally, we determined that DLA generally did not implement the DIACAP in accordance with DODI 8510.01."

- J6 does **not concur** with the DLA OIG's conclusion that DLA generally did not implement the DIACAP in accordance with DODI 8510.01. J6's nonconcurrence with the DLA IG's conclusion is based on a number of factors surrounding the actual audit that was conducted as well as evidentiary proof that the process is indeed implemented in accordance with DODI 8510.01 leveraging DODI 8500.2. The DLA OIG's audit included a review of selected IA controls assigned to five information systems in accordance with the DIACAP, so the audit was in actuality of specific information system's as opposed to the mechanics of the actual process. DLA's DIACAP implementation was documented in an implementation guide, complete with a full transition plan in 2008 and the DLA DIACAP Implementation Guide is a derivative of the DODI 8510.01, including every requirement documented in DODI 8510.01 for every step of the process. Additionally, DLA's DIACAP implementation as documented in the "DLA DIACAP Implementation Guide" was the subject of review by the DIACAP TAG Chairperson, and a full endorsement of this guide was given at that time. In addition to that, DLA's implementation of DIACAP is supplemented with an IA Control Validation Exercise component of the J61 managed IA Compliance Review Program, which provides onsite, in-person verification of IA controls compliance status' on a scheduled basis. While the DLA OIG's audit revealed instances where the application of IA control requirements where not fully met or subject to interpretation with regards to the IA controls implementation and compliance status, that was not sufficient basis for determining the implementation of the process to be insufficient.

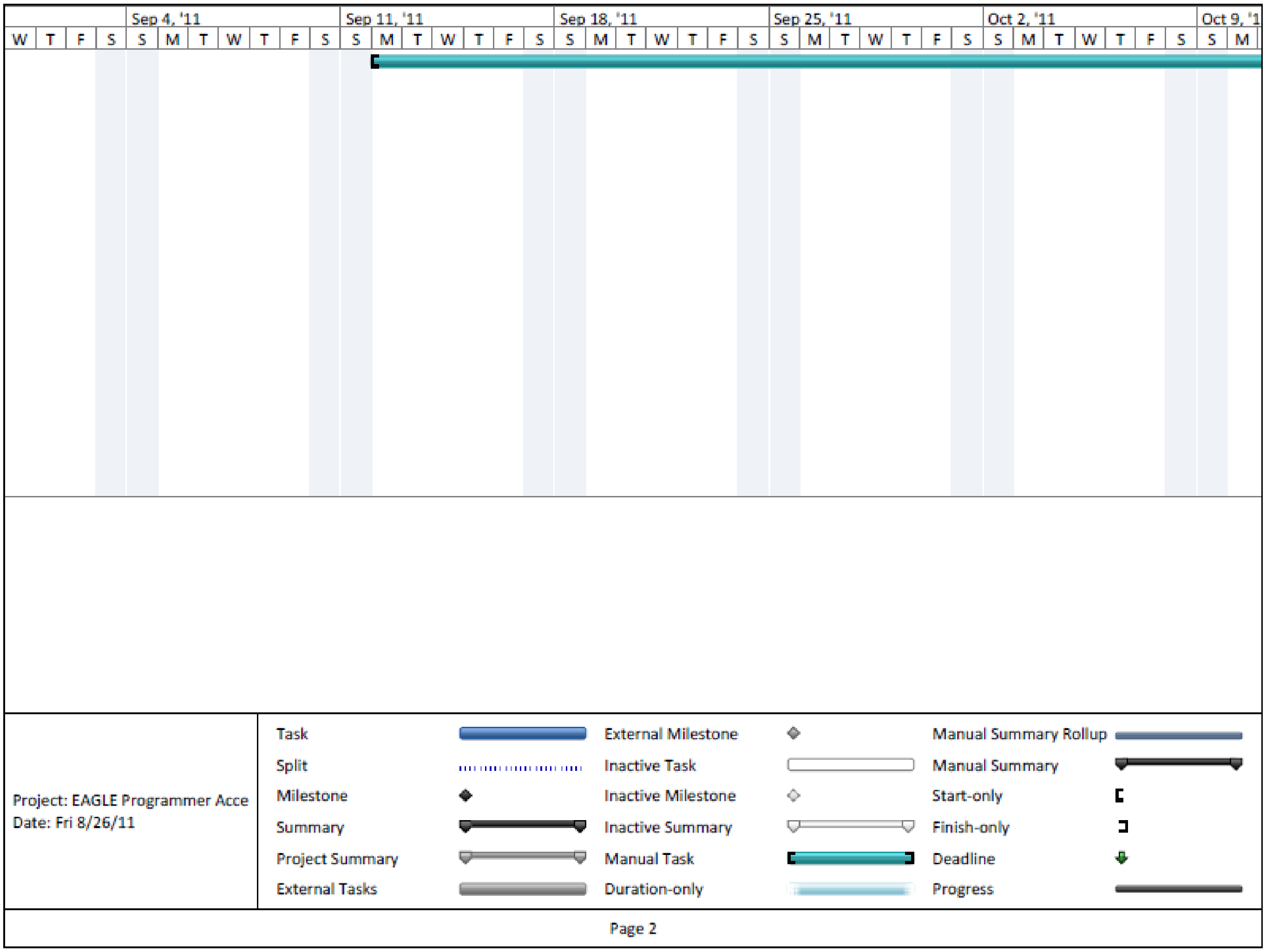


ID	ℹ	Task Name	Duration	Start	Finish	Predecessors	Aug 28, '11 S M T W
1		Research monitoring tools for production environment that can detect unauthorized changes	75 days	Mon 9/12/11	Fri 12/23/11		
2		Obtain approval for selected tool	30 days	Mon 1/2/12	Fri 2/10/12		
3		Acquire and install monitoring tool	55 days	Mon 2/13/12	Fri 4/27/12		
4		Test monitoring tool	35 days	Mon 4/30/12	Fri 6/15/12		
5		Install monitoring tool in production	45 days	Mon 6/25/12	Fri 8/24/12		
6		Secure monitoring tool and audit logs (system and database) from modification by EAGLE developers	15 days	Mon 8/6/12	Fri 8/24/12		
7		Perform review of baseline code and generate a checksum (checksum used to verify application integrity)	15 days	Mon 8/13/12	Fri 8/31/12		
8		Checksum maintained by J6O IAM and EAGLE PM	1 day	Fri 8/31/12	Fri 8/31/12		
9		Publish baseline code to production	1 day	Fri 8/31/12	Fri 8/31/12		
10							
11		Ongoing Procedures					
12		Review and approve application changes and generate a checksum before publishing to production					
13		Periodically review and document developer access to production					
14		Periodically review database audit logs					

Project: EAGLE Programmer Acce
Date: Fri 8/26/11

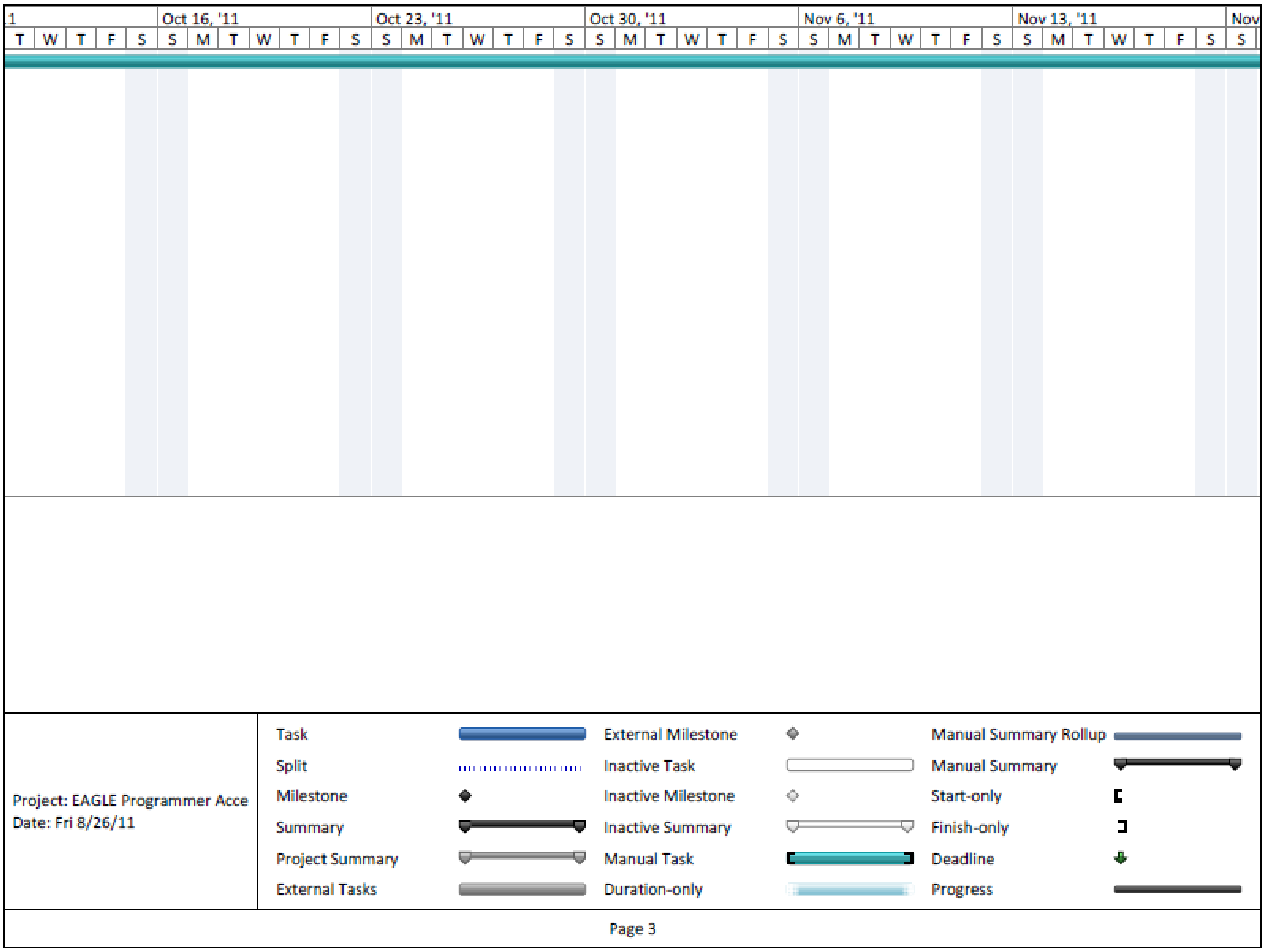
Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	⁞⁞⁞⁞⁞⁞	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Deadline	⇩
External Tasks	▬	Duration-only	▬	Progress	▬

Page 1



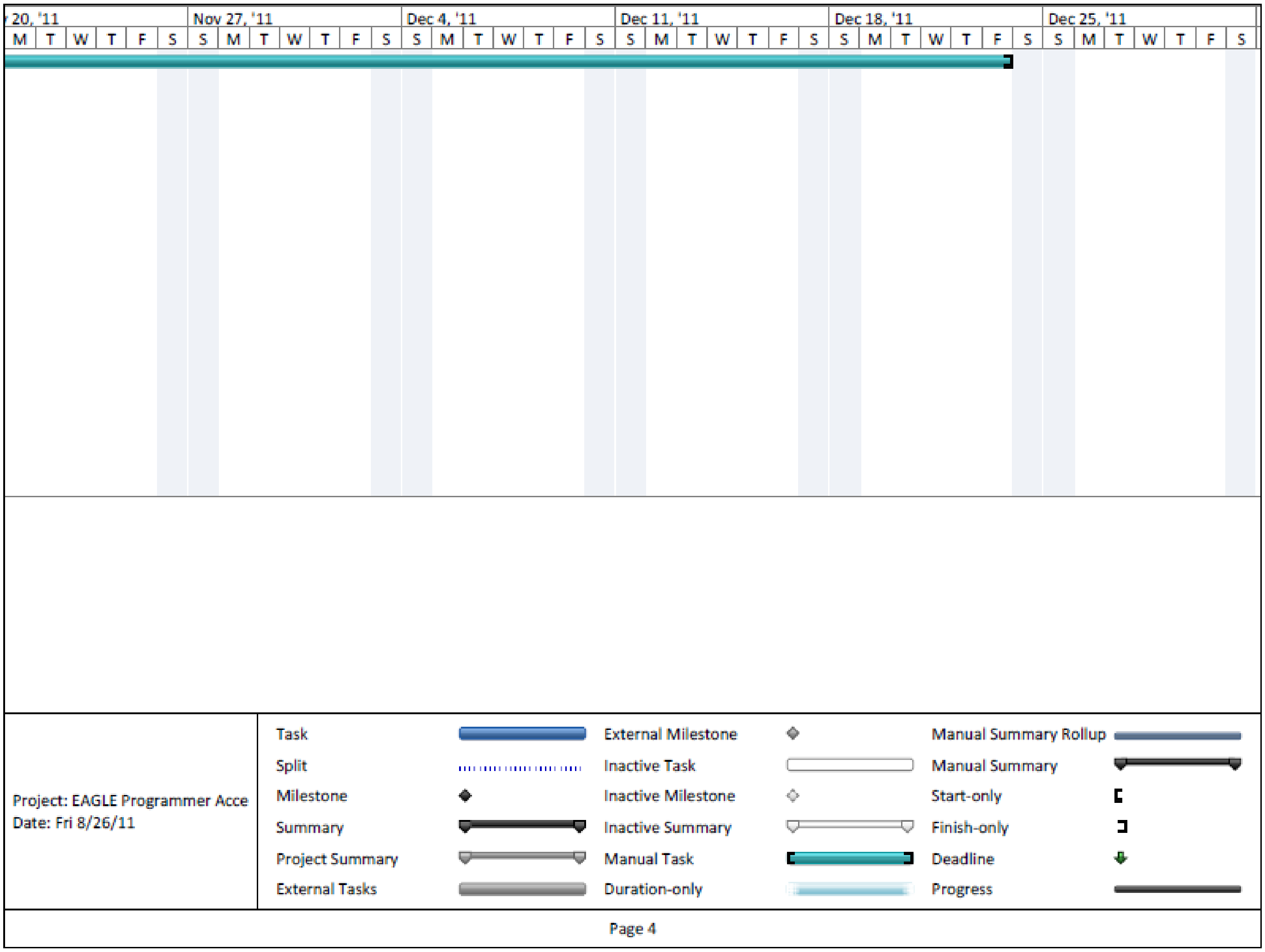
Project: EAGLE Programmer Acce
Date: Fri 8/26/11

Page 2



Project: EAGLE Programmer Acce
Date: Fri 8/26/11

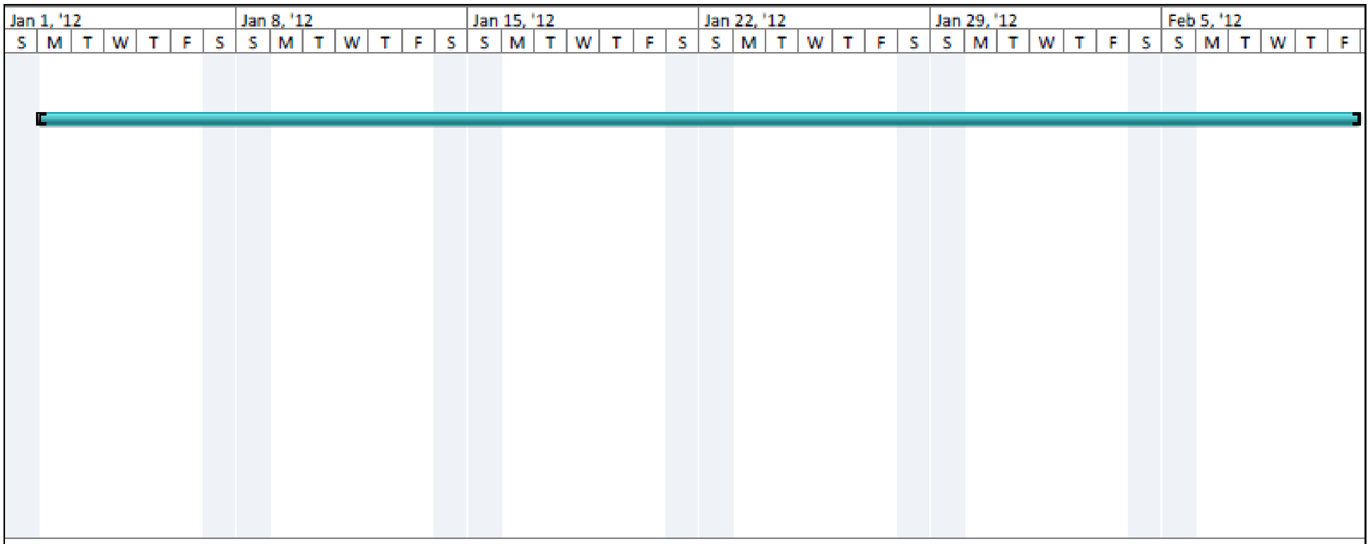
Page 3



Project: EAGLE Programmer Acce
Date: Fri 8/26/11

Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	┅	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Deadline	⬇
External Tasks	▬	Duration-only	▬	Progress	▬

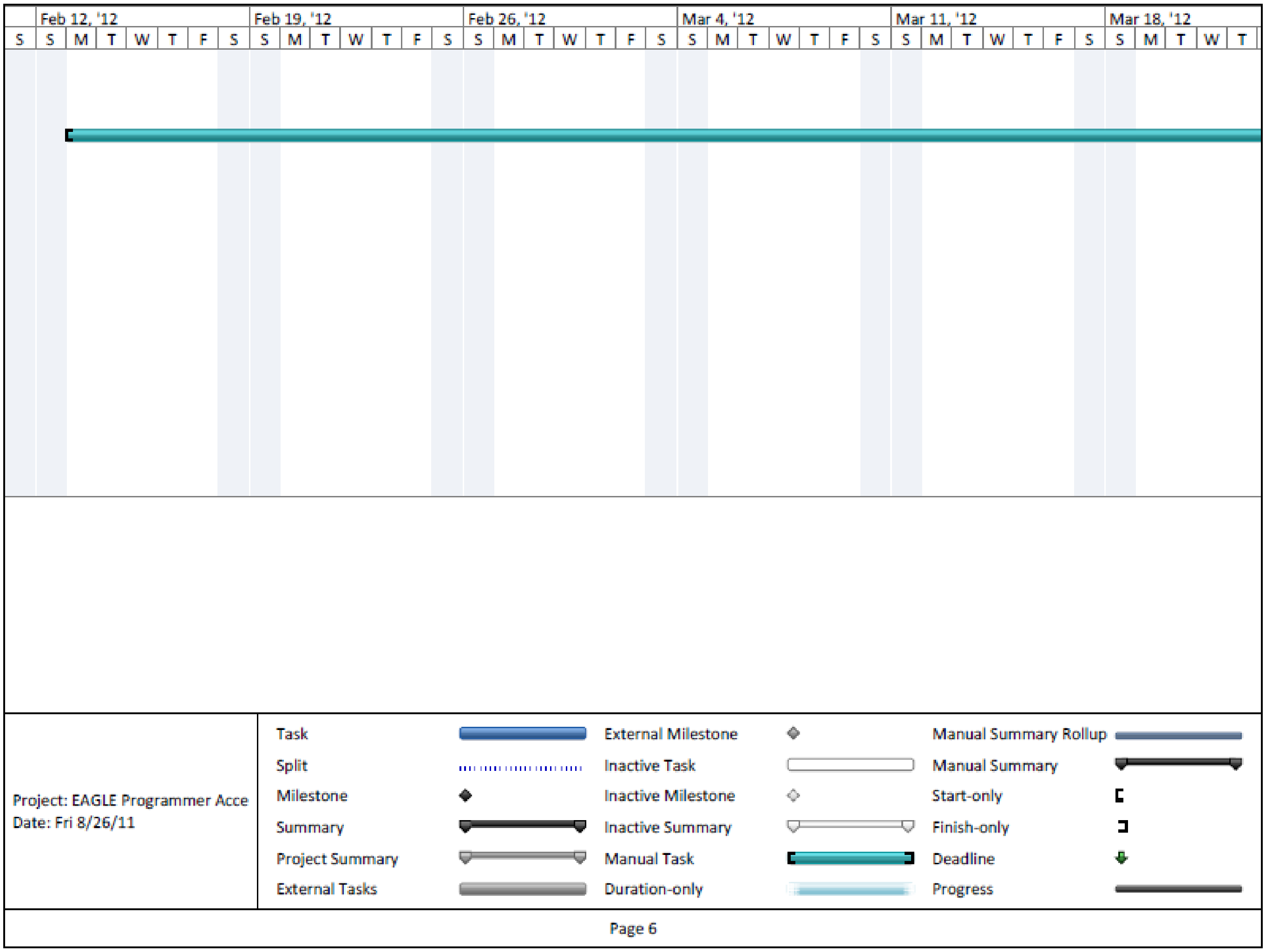
Page 4



Project: EAGLE Programmer Acce
Date: Fri 8/26/11

Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	┈┈┈	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Deadline	⇩
External Tasks	▬	Duration-only	▬	Progress	▬

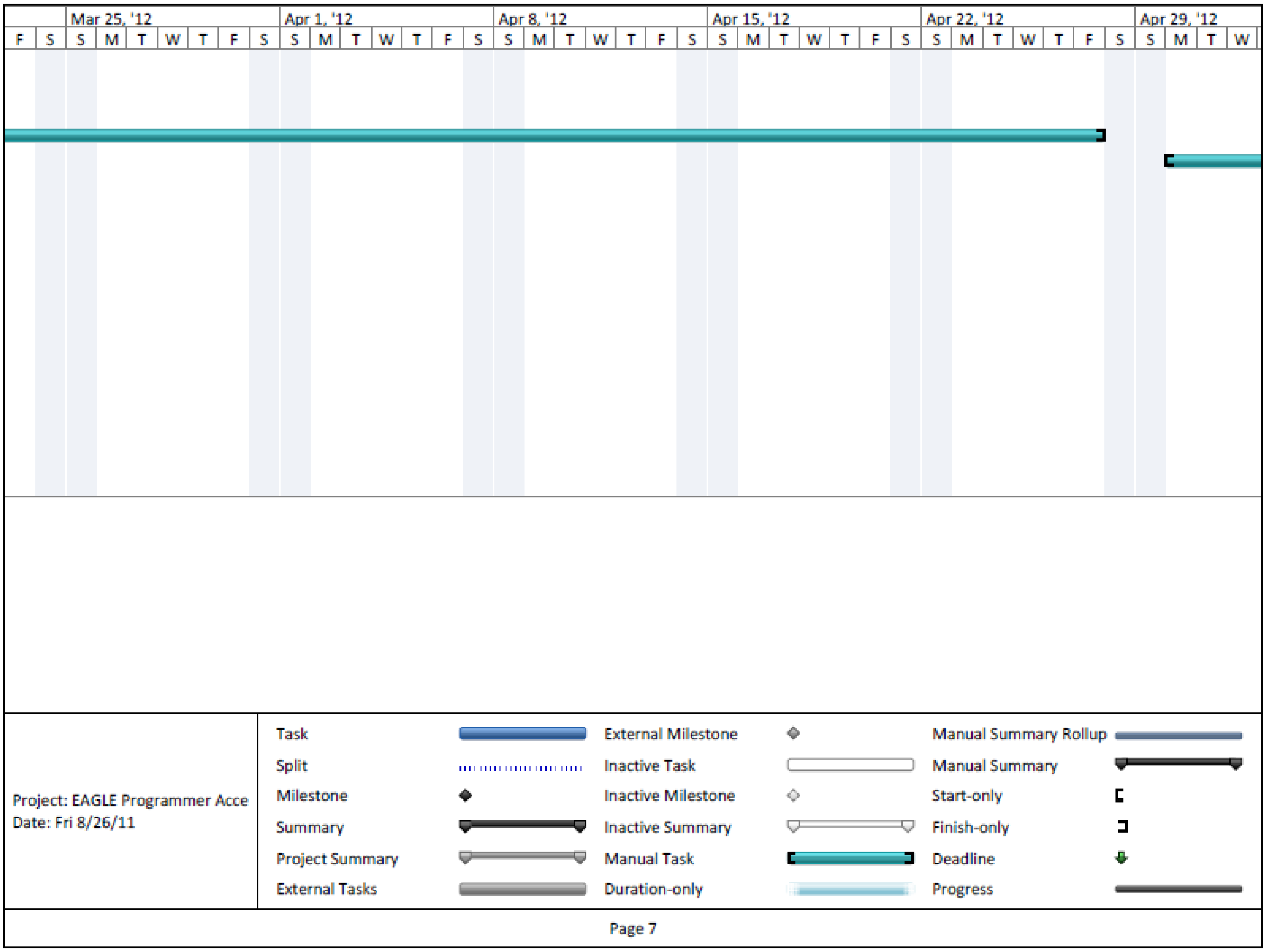
Page 5



Project: EAGLE Programmer Acce
Date: Fri 8/26/11

Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	┆┆┆┆┆┆	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Deadline	↓
External Tasks	▬	Duration-only	▬	Progress	▬

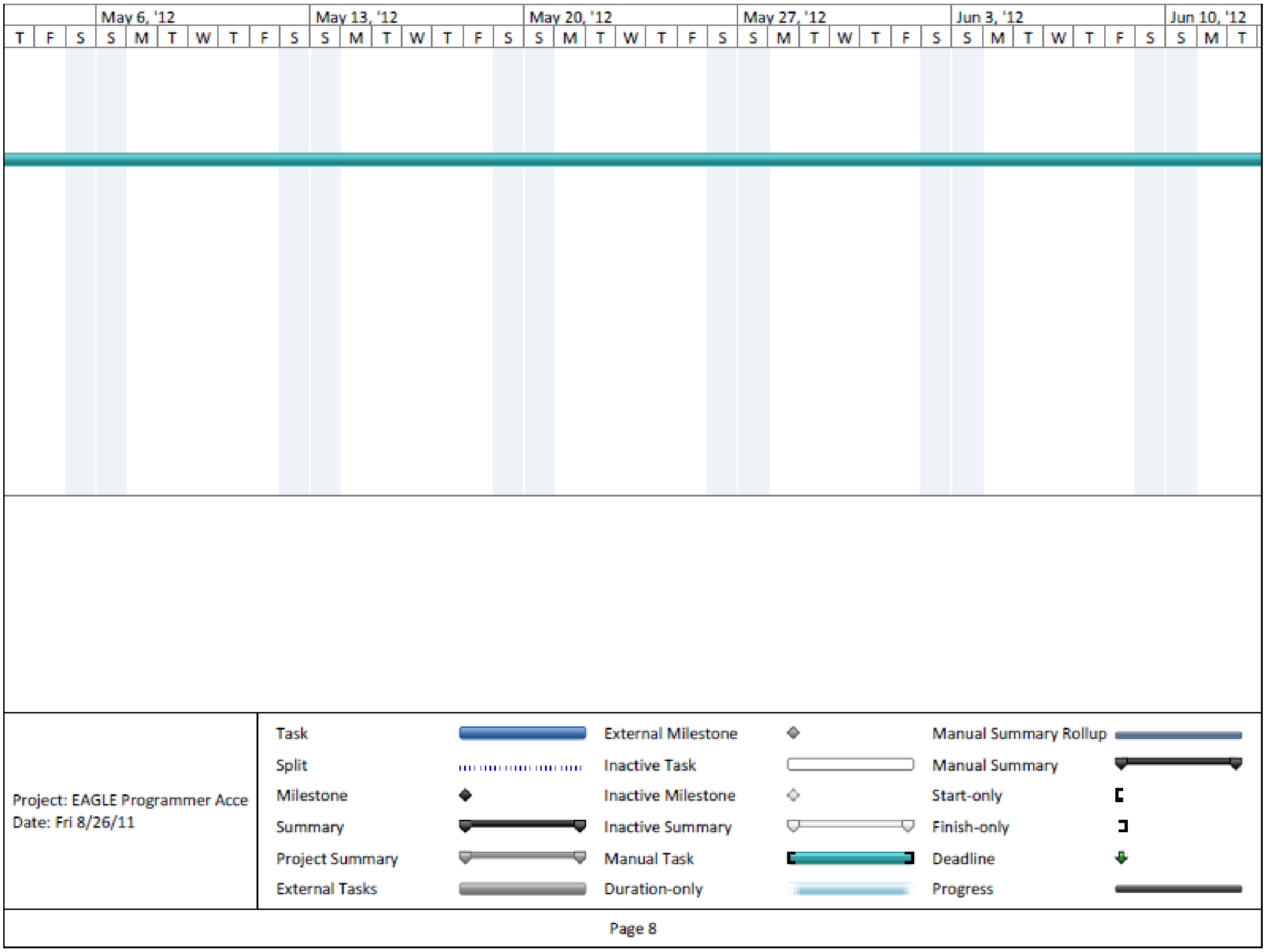
Page 6



Project: EAGLE Programmer Acce
Date: Fri 8/26/11

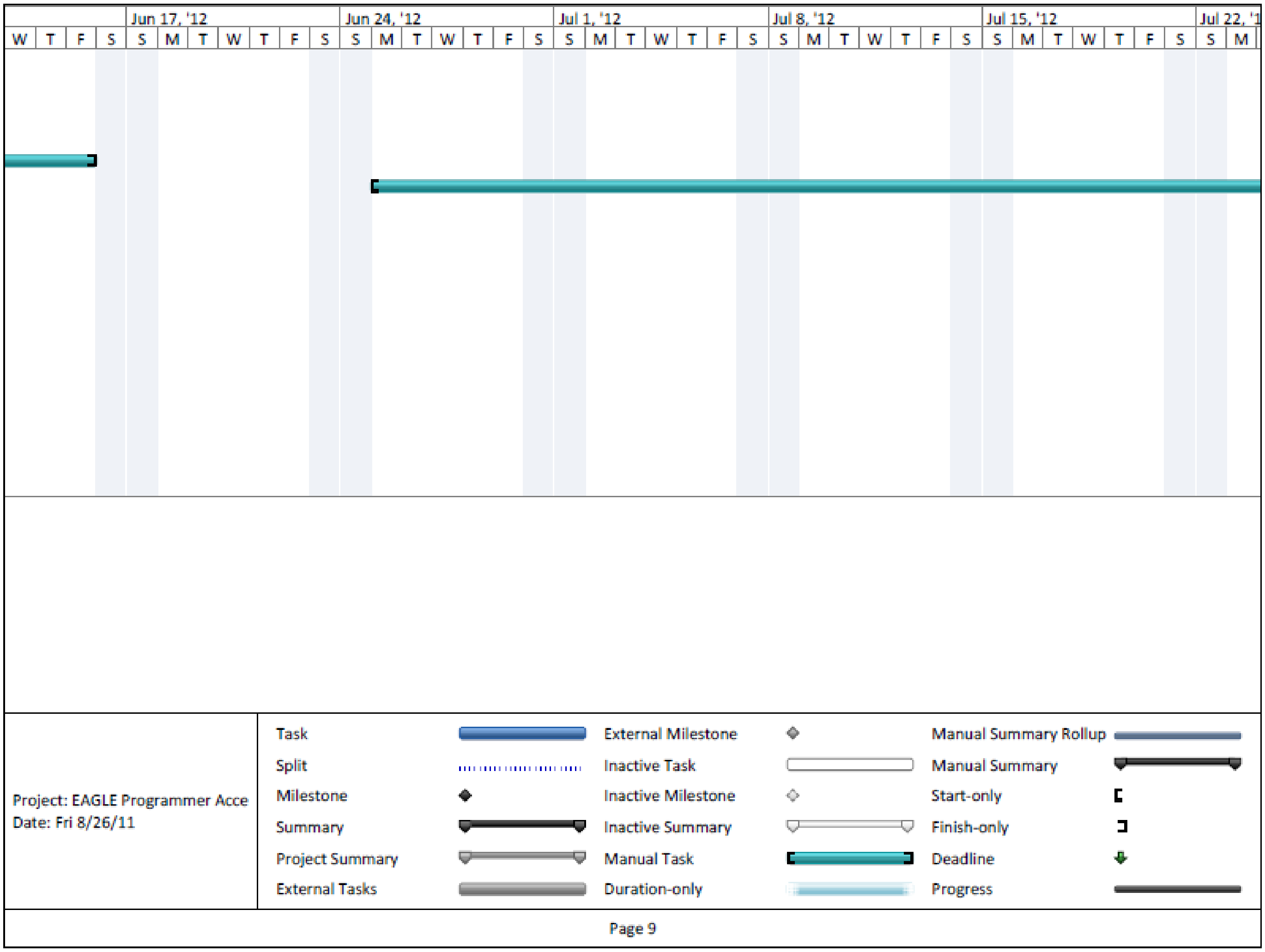
Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	┈	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Deadline	⇩
External Tasks	▬	Duration-only	▬	Progress	▬

Page 7



Project: EAGLE Programmer Acce
Date: Fri 8/26/11

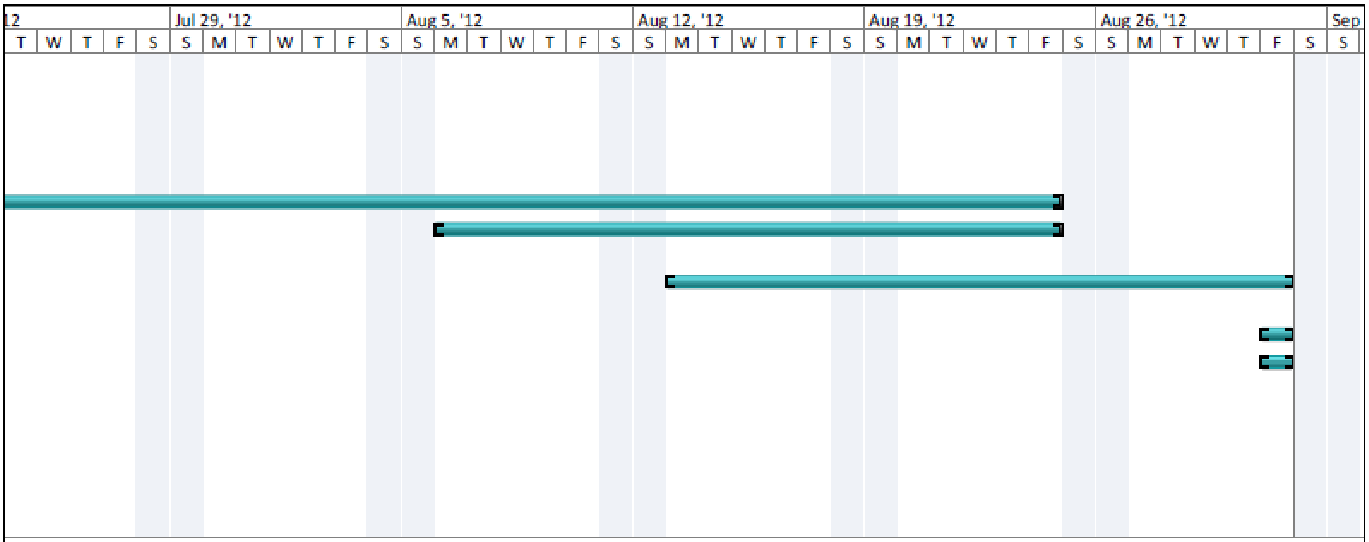
Page 8



Project: EAGLE Programmer Acce
Date: Fri 8/26/11

Task	▬	External Milestone	◆	Manual Summary Rollup	▬
Split	┈	Inactive Task	▭	Manual Summary	▬
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary	▬	Inactive Summary	▭	Finish-only	]
Project Summary	▬	Manual Task	▬	Deadline	⇩
External Tasks	▬	Duration-only	▬	Progress	▬

Page 9



Project: EAGLE Programmer Acce
Date: Fri 8/26/11

Task		External Milestone	◆	Manual Summary Rollup	
Split		Inactive Task	▭	Manual Summary	
Milestone	◆	Inactive Milestone	◇	Start-only	[
Summary		Inactive Summary		Finish-only	]
Project Summary		Manual Task		Deadline	⇩
External Tasks		Duration-only		Progress	

Page 10

On October 27, 2011, DLA Management provided DLA OIG with additional information on the corrective action plans and the estimated completion dates to implement the auditors' recommendations. Verbatim Management comments of the additional information were included below:

> **Recommendation 3**. **Conduct an evaluation of all applicable IA controls and assign baseline IA controls for each DLA system in Enterprise Mission Assurance Support System (eMASS) to include an accurate identification of inherited, shared, and DLA-owned IA controls.**
>
> **Response**. DLA OIG needs to clarify this recommendation and the actual finding. The recommendation is not totally clear in terms of what the auditors are attempting to identify as a deficiency, or what the recommendation requires of J6 that isn't already part of the DLA DIACAP implementation. Until this is done no action can be taken.
>
> The following recommendations need an estimated completion date (ECD):
>
> - **Recommendation 5. Coordinate with the Director of DLA to obtain the delegation of authority to update the DLA enterprise Service Support Document (ESSD) and SLAs with Defense Information systems Agency (DISA) to explicitly define the expected level of services and IA roles and responsibilities.**
>
>   **Response:** ECD: December 2012. These three recommendations (5/6/7) require DISA to update their internal SLA document templates. DLA has no authority to compel DISA to change their ESSD document template as it is another DOD Agency. This impacts not just DLA but all of DISA's customers. In fact, an ECD depends entirely on DISA revising their Service Level agreement process and documentation to be in line with IT industry best practices. DLA is one of the largest DISA customers and this effort must be coordinated across IG offices. DLA J6 would appreciate the additional support and coordination between DLA OIG and the DISA OIG. This would ensure our efforts can be completed in a timely manner.
>
>   **Recommendation 6. Coordinate with DISA to explicitly define listings of system-specific inherited, shared, and customer owned IA controls for all DISA hosed DLA systems.**
>
>   **Response.** ECD: December 2012**.** These three recommendations (5/6/7) require DISA to update their internal SLA document templates. DLA has no authority to compel DISA to change their ESSD document template as it is another DOD Agency. This impacts not just DLA but all of DISA's customers. In fact, an ECD depends entirely on DISA revising their Service Level agreement process and documentation to be in line with IT industry best practices. DLA is one of the largest DISA customers and this effort must be coordinated across IG offices. DLA J6 would appreciate the additional support and coordination between DLA OIG and the DISA OIG. This would ensure our efforts can be completed in a timely manner.
>
>   **Recommendation 7. Communicate guidance to the Director of DLA Information Operations at Ogden on the minimum information that must be reviewed and**

communicated back to DLA Information Operations to update SLAs with DISA on an annual basis.

Response. ECD: December 2012**.** DLA and DISA established a team to work with all DLA stakeholders to ensure communication is clear and all minimum information is received. SLAs are a part of the ESSD revision and DLA Information Operations at Ogden is included as a stakeholder.

- **Recommendation 11. Coordinate with DISA to obtain validation test results and applicable supporting artifacts for inherited IA controls.**

  Response. ECD: November 30, 2011

- **Recommendation 16. Develop and enforce an Agency-level policy and procedure for the account management process that include the granting, modifying, terminating, and recertifying of user accounts.**

  Response. ECD: December 2012. A J6 policy will be written that requires all access accounts be approved through AMPS. This policy will also address procedures for the account management process that includes the granting, modifying, terminating, and recertifying of user accounts.

- **Recommendation 17.** Develop and enforce the following:
  - **Policies and procedures for proper retention and completion of the system access authorization request that contain specific instructions, including required blocks of the form/data fields that must be completed for each type of system access request (ie., authorized, privilege, modification to current role, recertification, termination, etc.) and**
  - **A mechanism to monitor compliance with the agency-wide account management process.**

  Response. ECD: December 2012. A J6 policy will be written that requires all access accounts be approved through AMPS. This policy will address proper retention and completion of the system access authorization request that contains specific instruction, including required blocks of the for/data fields that must be completed for each type of system access request and also develop a mechanism to monitor compliance.

- **Recommendation 18. Enforce the requirement that all EBS users only are granted access or current roles be modified through AMPS and complete the AMPS revalidation of users converted from the legacy account provisioning application.**

  Response. ECD: December 2012. While it is implied that AMPS will be used to access EBS no official J6 policy currently exists. A J6 policy will be written to enforce all system access accounts be approved through AMPS. The AMPS revalidation of users converted from the legacy account provisioning application is complete.

- **Recommendation 22. Centralize the administration of DSS user provisioning, modification, disabling, and termination to enhance management oversight of user accounts by the IAO.**

  Response. ECD: November 2011. DLA Information Operations at New Cumberland agrees with the comment and will cut over to a centralized DSS account administration methodology concurrent with the west RACF cutover. As the groundwork is in place with DSS accounts at DECC-M, final action entails re-routing 2875 requests for DSS DECC-O through the same process. .

- **Recommendation 28. Develop a policy and procedure requiring a definition of what constitutes an internal and external user to DLA for each system. In addition, document in the system access policy for each DLA system the IA awareness training and security clearance verification requirements for the defined internal and external users.**

  Response. ECD: June 2012. DLA Information Operations (J64) has drafted a DLA Instruction, Enterprise Remote Access Policy and Procedures. This draft DLA Instruction does not currently address internal or external users but will be modified to include definitions of both.

  The IA Awareness training is tracked through DLA's Learning Management System (LMS) and verified through the Account Management and Provisioning System (AMPS) by the information Assurance Managers. As part of the DLA LAN account annual validation, AMPS checks to ensure that the user has completed the IA Awareness training within the last year. Any employee or contractor who accesses a DLA system must have a current adjudicated investigation before granted access. The access is requested on a system Authorization Access Request (SAAR) and the IT level and security investigation is verified by the Security Representatives.

- **Recommendation 29. Coordinate with the subject matter experts to establish listings of available user functions/roles for BSM-E and PORTS.**

  Response. ECD: June 2014. This is being worked on as part of Energy Convergence full deployment as recommended by OIG and agreed upon.

- **Recommendation 30. Coordinate with the subject matter experts to establish listings of the permissible/not-permissible combination of functions/roles for BSM-E, PORTS, and DFAMS.**

  Response. ECD: June 2014. This is being worked on as part of Energy Convergence full deployment as recommended by OIG and agreed upon.

- **Recommendation 31. Ensure the established listings of available user functions/roles and permissible/not-permissible combination of functions/roles that are critical to protecting DLA Energy systems be incorporated in the Energy Convergence system requirements and system documentation.**

  Response. ECD: June 2014. This is being worked on as part of Energy Convergence full deployment as recommended by OIG and agreed upon.

- **Recommendation 32. Establish a formal Disaster Recovery/COOP Training Program across the DLA enterprise for recovery team personnel.**

  Response. ECD: June 2012. Training program established September 2010. On-going training as COOP Planners change. The draft IT COOP Instruction includes this training requirement. The instruction is going through final review.

- **Recommendation E1. Coordinate with the Director DLA Informations Operations to formally establish an EAGLE CCB Charter**

  Response. Completed October 2011.

- **Recommendation E2. Update the EAGLE CM policies and procedures to reflect the roles and responsibilities of the chartered EAGLE CCB.**

  Response. Completed March 2011.

- **Recommendation E3. Enforce the updated EAGLE Configuration Management (CM) policies and procedure to ensure a comprehensive CM process, which would also include the requirement for completing and retaining CM documentation.**

  Response. Completed March 2011.

- **Recommendation H1. Update the DSS CCB charter to designate at a minimum the IAM as an advisory member, and enforce the requirement of periodic audit of InfoMan records to ensure compliance with the software Configuration Management Plan for DSS.**

  Response. ECD: January 2012. DLA Information Operations at New Cumberland agrees with the recommendation and will revise the DSS CCB Charter to include, by name, the IAM as an advisory member. The IAM is now included in appropriate DSS meetings. HQ J64 will complete the staffing of the DSS charterand facilitate final staff action and signatures. In the interim and until the chater is signed, the IAM will be invited as a guest advisor to DSS CCB meetings. The draft charter is in final staffing/coordination. Additionally, periodic audits of InfoMan records to ensure compliance with the Software Configuration Management Plan for DSS will begin in the fourth quarter 2011. While the current DSS configuration management methodology aligns with DLA 8250.4, we are reevaluating the methodology against DLA 8250.4 and will adjust the methodology as necessary to ensure compliance.

The following recommendations need a description of the corrective actions performed/will be performed and the ECD.

- **Recommendation F3. Develop and implement a formal procedure detailing the documentation requirements for the following:**
    - **Changes that moved to production but did not successfully progress through the normal CM process (i.e., functional testing, QA testing, etc.) and**
    - **The types of documentation required (i.e., SCA approval, QA results, etc.) prior to changes being moved to production.**

    Response. The DLA Logistics Information Service TSC Change and Configuration Management User Guide was updated to include the types of documentation required. CLOSED; September 2011. All programs not being migrated to production were cleaned up. CLOSED, June 2011.

- **Recommendation F4. Coordinate with DISA to perform an inventory of the programs residing in the FLIS Mainframe staging environment and remove programs if they will not be migrated to production.**

    Response. DLIS manually updated all Change Requests (Application Info: field within the Task Order Web Site (TOWS)) to reflect that they are FLIS application changes. A Change Request was initiated to add a drop down menu to the Application Info: Field within the TOWS that identifies all applications that are utilized in DLIS and DLA Disposition Services. Furthermore, this field will be identified as “Mandatory” to ensure this error does not occur again. Change Request number is 2011-272-001 with sub-task number OT8235. Service Desk Express has always had applications properly identified. CLOSED: October 2011.

- **Recommendation F5. Coordinate with DISA to review and inventory the FLIS Mainframe production program libraries and remove programs that are no longer needed.**

    Response. As the post implementation release notice is received, the System Change Request (SCR) Administrator will conduct a reconciliation of those change requests that were implemented within the TOWS. This is done to ensure that the TOWS reflect what was accomplished with the movement of the CRs. This procedure is now documented within the change Request User Guide. The Software Change Administrator conducted an audit of the Pre/Post release notice. CLOSED: September 2011.

    The PM is currently developing a CR to delete programs that are no longer needed. ECD: April 2012.