Director, Operational Test and Evaluation

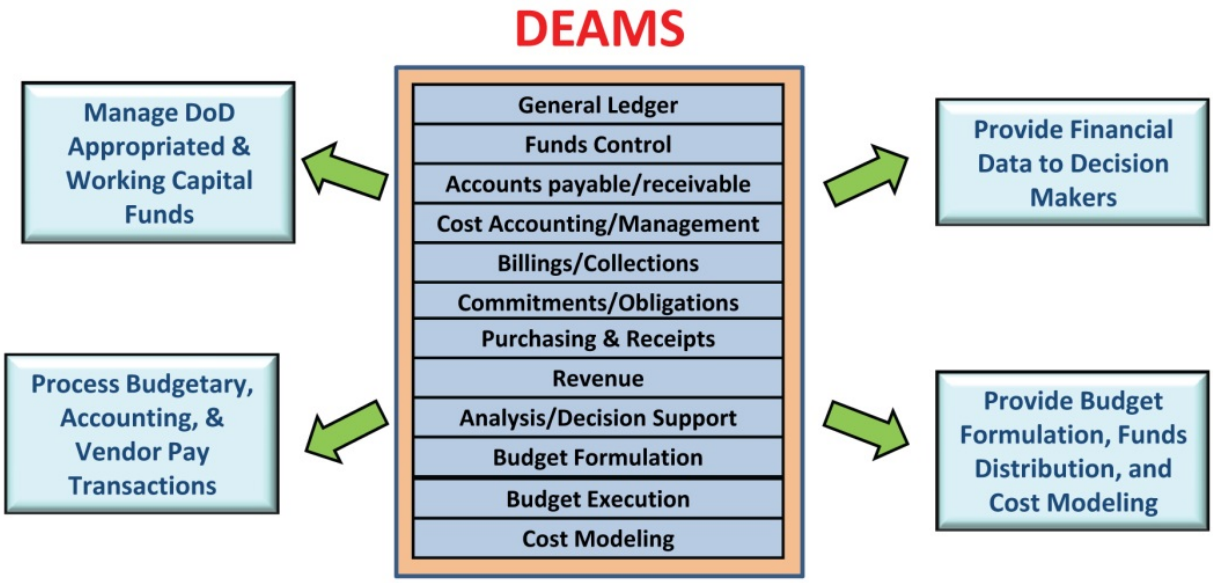
Defense Enterprise Accounting and Management System (DEAMS)

Increment 1 Release 3 Initial Operational Test and Evaluation Report

August 2015

This report on the Defense Enterprise Accounting and Management System (DEAMS) fulfills the provisions of Title 10, United States Code, Section 2399. It assesses the adequacy of testing and the operational effectiveness, operational suitability, and cybersecurity posture of the DEAMS.

J. Michael Gilmore
Director



Defense Enterprise Accounting and Management System (DEAMS)

Executive Summary

This report assesses the adequacy of the Defense Enterprise Accounting and Management System (DEAMS) Increment 1 Release 3 Initial Operational Test and Evaluation (IOT&E) and the system's operational effectiveness, operational suitability, and cybersecurity. The Air Force Operational Test and Evaluation Center (AFOTEC) conducted the IOT&E between October 1, 2014, and May 29, 2015, at seven bases that included three Air Force major commands, three U.S. Combatant Commands, and the Defense Finance and Accounting Service (DFAS). Additionally, Army and Air Force cybersecurity teams conducted a cooperative vulnerability and penetration assessment at Gunter Annex, Montgomery, Alabama, and an adversarial assessment at McConnell Air Force Base (AFB), Kansas.

Adequacy of IOT&E

The IOT&E was adequate and was executed in accordance with the Test and Evaluation Master Plan (TEMP) and the IOT&E plan, both of which were approved by DOT&E. AFOTEC developed 40 Measures of Effectiveness and Suitability to resolve three Critical Operational Issues, nine Key Performance Parameters, and other effectiveness and suitability parameters documented in the TEMP. Because DEAMS had been in operational use for more than five years and the test environment was live with actual users, AFOTEC had no direct control over the sample sizes. AFOTEC mitigated this limitation by spreading the IOT&E over several months to collect necessary data determined by the Design of Experiments (DOE) to provide a statistical confidence level of 80 percent. The IOT&E test plan was informed by two previous operational assessments and continually refined by AFOTEC, the functional management office, and the program management office. The Program Executive Officer (PEO) halted testing twice to allow users to reduce transaction backlogs that were building up and causing difficulties with DEAMS usability and the operational test; this delay did not affect the adequacy of testing. Cybersecurity testing was done in accordance with DOT&E policy and DOT&E-approved test plans. The Joint Interoperability Test Command evaluated the system's interoperability with other systems and has published a separate interoperability assessment.

Effectiveness

During the IOT&E, DEAMS was not operationally effective. DEAMS had shown progress towards operational effectiveness during the second operational assessment (OA2) in 2014; however, a software change between OA2 and IOT&E to support end-of-year accounting closeout affected DEAMS operational performance during the IOT&E. DEAMS successfully prevented users from exceeding budget targets and correctly computed capitalization and depreciation of assets. The system employed the Standard Financial Information Structure and consistently reconciled subsidiary accounts to the General Ledger. However, DEAMS did not effectively perform several critical accounting and management functions, the following four of which are Key Performance Parameters (KPP):

- DEAMS did not provide a reliably correct balance of available funds.
- At the end of Fiscal Year (FY) 2014, DEAMS was unable to close end-of-year accounts within the timeframe prescribed by the Air Force. No accounts were successfully closed by the prescribed date at the four bases that the test team visited in October 2014. During the closeout:
  - A General Ledger stopped updating
  - Final account balances could not be validated
  - An Open Document List was inaccurate
  - A Status of Funds could not be pulled in a timely manner
  - Transaction statuses could not be confirmed
  - A selective transaction history was unavailable to back up the Status of Funds
- Some DEAMS users characterized the 2014 Fiscal Year-End (FYE) closeout as the worst FYE closeout.
- During the remaining period of the IOT&E, DEAMS did not meet the 95 percent thresholds for balancing end-of-quarter and end-of-month accounts.
- DEAMS did not record transactions in a timely manner. At one point during the test, over 3,000 travel transactions and 9,400 fuel bills were past the 24-hour timeliness threshold and had not been recorded in DEAMS. A backlog of transactions resulted in an increase in late penalty payments to $465.74 per $1 Million ($1M) in January 2015, which was nearly 10 times the Air Force's FY15 goal of $49.00 per $1M.
- DEAMS did not meet the 98 percent threshold for balancing with Treasury funds. It was within 0.5 percent of the threshold; however, the total dollar variance had increased by $15M over the course of the IOT&E, indicating a possible systemic issue with maintaining proper balances with Treasury. The upcoming increase in DEAMS users from 5,000 to 29,000 may exacerbate this problem unless it is addressed.

Some enhancements to DEAMS intended to correct defects noted during previous operational assessments were not fielded in time for the IOT&E. The most significant of these was Oracle Business Intelligence Enterprise Edition (OBIEE) software that was purchased to replace Discoverer, the current DEAMS reporting tool. OA2 found Discoverer to be an unsatisfactory system. OBIEE was not deployed during IOT&E because deficiencies found during developmental testing. During IOT&E, about half of the respondents (32 of 67) to a survey question on budget analysis and planning indicated dissatisfaction with DEAMS reporting capabilities, commenting that they relied on legacy systems for reporting rather than using Discoverer. This level of dissatisfaction is unchanged from previous operational testing. Users cited poor information quality, lack of timeliness, and difficulty in using Discoverer. During the IOT&E, only 69 percent of reports and queries (78 of 113) were correct.

Suitability

DEAMS was not operationally suitable. The system met its hardware reliability, availability, and maintainability suitability requirements, demonstrating an operational availability (A_o) of 98.1 percent, which exceeded the 98 percent threshold for A_o (the 80 percent confidence interval ranged from 96.0 to 98.8 percent). DEAMS did not meet Net-Ready KPP requirements for the exchange of critical information. Furthermore, DEAMS exhibited problems with software reliability growth as measured by the increase in the amount of deficiencies during IOT&E including many high severity deficiencies (Severity-2) that have remained unresolved for 240 days or longer.

- The number of high severity Incident Reports increased from 33 at the start of the test to 81 by the end of the test.
- The DEAMS functional management office reported 65 outstanding Severity-2 defects at end of test. Twenty of these were more than 240 days old.
- The DEAMS functional management office reported 50 outstanding Severity-2 Software Change Requests at end of test. Thirty-five of these were more than 240 days old.

The Program Management Office (PMO) did not follow its own configuration management procedures for developmental testing. That procedure prescribes the conduct of system integration testing and regression testing before placing new software in the production environment. Rather than choosing to delay the scheduled IOT&E, which began on October 1, 2014, the PEO decided to field the Fiscal Year-End portion of sub-release 3.2 although none of the software had completed the defined developmental testing process. The PEO maintained the original IOT&E schedule in order to test the ability of the DEAMS to perform fiscal year end account closing.

The new software failed to perform the FYE closings within the timeframe prescribed by the Air Force. In addition, introducing sub-release 3.2 software into the live environment without properly performing regression testing affected the fielded DEAMS software. Other types of transactions began to fail, causing the PEO, with DOT&E concurrence, to temporarily halt processing these transactions in DEAMS. Substantial backlogs developed and the PEO decided to suspend IOT&E until the backlogs and software deficiencies could be addressed. Four months later, the IOT&E resumed on February 17, 2015. However, backlogs still adversely affected DEAMS usability, so the PEO suspended testing for another month, with DOT&E concurrence. The IOT&E ended on May 29, 2015, with substantial transaction backlogs still present.

DEAMS training, while demonstrating gradual improvement since the last operational assessment, did not prepare users to effectively employ DEAMS. The testers found that many new users had very little knowledge of DEAMS. Some users only accessed DEAMS sporadically and did not develop or maintain proficiency. A long time gap between initial training and live deployment also degraded user proficiency because users forgot much of what they had learned.

Cybersecurity

DEAMS was not survivable. Adversarial Assessment cybersecurity testing showed that the system did not protect its information or detect cybersecurity threats. In February 2014, the Air Force's 177th Aggressor Squadron conducted a cyber-economic vulnerability assessment of DEAMS that revealed serious cyber vulnerabilities. DOT&E made several recommendations for mitigating these vulnerabilities in a classified test report. From 9 – 13 February 2015, Army Research Laboratory conducted a cooperative vulnerability and penetration assessment of DEAMS and noted vulnerabilities similar to those found during the 2014 cyber-economic vulnerability assessment. Following the cooperative assessment, AFOTEC and the 177th Information Aggressor Squadron conducted an adversarial assessment and achieved the same results that they had during the 2014 cyber-economic vulnerability assessment, using similar means. Further cybersecurity results and recommendations are contained in the classified cybersecurity annex to this report.

Interoperability

The Joint Interoperability Test Command (JITC) conducted an Interoperability Assessment of the DEAMS based on the data from August 2014 through May 2015. JITC collected data and assessed DEAMS in the Global Combat Support System – Air Force (GCSS-AF) production environment located at Maxwell AFB – Gunter Annex, Montgomery, Alabama. The results of the assessment demonstrated that 5 of the 22 available critical interfaces did not meet the required information exchange requirements.

Key Performance Parameters

Table 1 shows the test results for the Measures of Effectiveness (MOEs) and Measures of Suitability (MOSs) that define the DEAMS KPPs. The criteria were not met for four of seven Operational Effectiveness KPP MOEs. The criteria were not met for three of six Operational Suitability KPP MOSs while two KPP MOSs were not resolved due to a lack of data. Table 1 also includes the confidence intervals (CI) for the results, where applicable, based on an 80 percent level of confidence.[1] DEAMS nearly achieved its 98 percent threshold for MOE 2.3, Balance with Treasury; although the absolute dollar variance value increased by $135.8M to $150.7M from October to April 2015, indicating that there may have been systemic issues with maintaining proper balances with Treasury.

[1] The DEAMS requirements document shows the Net-Ready KPP as a single KPP that comprises both interoperability and information assurance. However, the DOD now defines the Net-Ready KPP only in terms of interoperability so cybersecurity (formerly information assurance) and its four MOSs are treated separately from the Net-Ready KPP in this report.

Table 1. IOT&E Results for DEAMS Key Performance Parameters

COI	KPP	Criterion	Threshold	Attempts	Successes	Result	Confidence Interval	Assessment
COI 1. Does DEAMS enable decision support? (Operational Effectiveness)	6	MOE 1.4 Time to Record Transactions	.95 ≤ 24 hrs	112	107	.94 ≤ 24 hrs	(.92, .97)	Not met. Substantial backlogs found.
	3	MOE 1.5 Accurate Balances	≥.98	119	84	.706	(.65, .76)	Not met
	2	MOE 1.6 Budget Control Targets not Exceeded	≥.98	10,744	10,744	1.0	N/A	Met
COI 2. Does DEAMS support financial operations? (Operational Effectiveness)	1	MOE 2.3 Balance with Treasury	≥.98	1,414,442	1,379,662	.975	N/A	Not met. Total dollar variance increased.
	5	MOE 2.4 Accounts Reconciled with General Ledger	≥.95	6	6	100	N/A	Met
	4	MOE 2.7 Invalid Data not Entered	≤.02	152,393	2,974	0	(.019, .020)	Met
	7	MOE 2.18 Period-end Closings (End of Month, Quarter, Year)	.95 EOM .95 EOQ .95 EOY	44,749 38,316 4	40,621 34,801 0	.908 .908 0	(.906, .909) (.906, .910) N/A	Not met
COI 3. Does DEAMS system management support financial management operations? (Operational Suitability)	8	MOS 3.5 Net Ready and Transfer of Information	1.0	N/A	N/A	0.77	N/A	5 of 22 critical interfaces did not meet JITC NR-KPP requirements
	9	MOS 3.6 Availability (Ao)	≥.98	308 hrs uptime / 314 total hrs		.981	(.97, .99)	Met
	8	MOS 3.1 Protection of Information	See classified reports					
	8	MOS 3.2 Detection of Intrusions	See classified reports					
	8	MOS 3.3 Response to Incidents	No data					
	8	MOS 3.4 Restoration of Functions	No data					

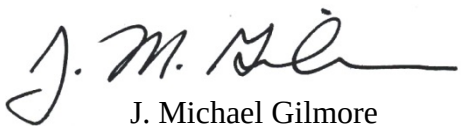
CI = Confidence Interval
COI = Critical Operational Issue

Recommendations

The Air Force should implement the following recommendations to support the successful fielding of DEAMS Increment 1.

- Identify processes, procedures, and/or software improvements to clear the transaction backlog, which will fix the lag time between transaction and posting, to ensure accurate and timely reporting.
- Work with DFAS to identify the root causes of imbalances between DEAMS and Treasury and change policies and procedures and/or implement software improvements to prevent further imbalances.
- Conduct robust regression testing to improve DEAMS performance and identify potential interface issues before fielding software updates and releases.
- Fix, or effectively mitigate, the deficiencies and cybersecurity vulnerabilities found during the IOT&E, as discussed in the classified appendix.

- Ensure that user training prepares users to use DEAMS at go-live and retain capabilities necessary to effectively use DEAMS.
- AFOTEC should conduct an FOT&E to verify that deficiencies found during the IOT&E are corrected and to determine whether the OBIEE reporting tool is operationally effective, suitable, and cyber-secure. Follow-on testing should include a repeat of the cyber vulnerability and penetration assessment to verify the fixes and mitigations for cybersecurity vulnerabilities.



J. Michael Gilmore
Director

Contents

This page intentionally left blank.

Section One
System Overview

The Defense Enterprise Accounting and Management System (DEAMS) is a Major Automated Information System that uses commercial off-the-shelf Enterprise Resource Planning software to provide accounting and management services for the Air Force; Air Force base tenant organizations; Headquarters, U.S. Transportation Command (USTRANSCOM); and the Defense Finance and Accounting Service (DFAS). DEAMS is intended to improve financial accountability by providing a single, standard, automated financial management system that is compliant with the Chief Financial Officer's Act of 1990 and other mandates. DEAMS performs the following core accounting functions:

- Core Financial System Management
- General Ledger Management
- Funds Management
- Payment Management
- Receivable Management
- Cost Management
- Reporting

When fully implemented throughout the Air Force, DEAMS will support guidelines established by the Office of Management and Budget and adhere to Financial System Integration Office Core Financial System Requirements. According to the DEAMS Program Manager, the Air Force now estimates the total program cost of DEAMS at $1.8 Billion, of which nearly $500 Million ($500M) was spent before Fiscal Year (FY) 2014.[2]

DEAMS Release 3 provides new capabilities, correcting previously noted deficiencies, and improving post-production maintenance. Air Force aimed efforts at achieving operational performance requirements, improving infrastructure and technical performance, testing and deploying baseline multi-base processes, and accomplishing business process optimization. Specific new planned capabilities included a replacement report generation tool, an update to the Standard Financial Information Structure (SFIS), customized error messages for designated users, improved interface handling, an enhanced interface with the Defense Departmental Reporting System (DDRS), and a capability for invoicing non-Federal customers for reimbursable activities. For the first time, DEAMS Release 3 provided capabilities to Air Force major commands beyond Air Mobility Command (AMC) and to U.S. Combatant Commands.

[2] DEAMS Program Manager, briefing to the Configuration Steering Board and Air Force Review Board, July 15, 2015

Background

DEAMS entered the acquisition cycle at Milestone A in 2005 as a Technical Demonstration of a basic Commitment Accounting capability at Scott Air Force Base (AFB), Illinois. The Air Force subsequently developed nearly 300 additional General Accounting capabilities and fielded them in May 2010 to about 1,100 users at Headquarters, USTRANSCOM and Headquarters, AMC at Scott AFB; DFAS Limestone, Maine; and a few Reserve Component locations. Following a Milestone B decision in January 2012, the DEAMS Program Management Office (PMO) began a series of corrective actions to resolve outstanding high severity defects in preparation for an operational assessment (OA1), which Air Force Operational Test and Evaluation Center (AFOTEC) conducted in July 2012. The results of OA1 demonstrated that DEAMS was not making satisfactory progress toward operational effectiveness, suitability and survivability.

Following OA1, the PMO continued to correct deficiencies and initiated a new fielding strategy. The PMO fielded the software to additional AMC bases without converting any legacy data. Users entered all new funding transactions into DEAMS, but continued to use legacy systems for transactions against prior year funding. The PMO also developed a new configuration management process and began to focus training on skills that would be needed by specific groups of users.

During 2013, the PMO, the Functional Management Office (FMO), and the Air Force Comptroller Financial Management Office continued to implement new DEAMS capabilities. The Air Force updated the DEAMS requirements document and periodically issued new software releases as subsets of Release 2. In September 2013, AFOTEC and DOT&E conducted an initial "quick look" before executing the last operational assessment (OA2) that included a limited evaluation of the Release 2 software that had been fielded to that point. During OA2, configuration management and documentation of workarounds had improved, but the number of system defects and the time required for the PMO to generate and promulgate user-approved and documented workarounds remained excessive. Many high-severity defects remained open and several new capabilities and enhancements still needed to be implemented to achieve operational effectiveness. System training was still inadequate – with the exception of DFAS training – and sufficient on-site technical support was lacking. The PMO continued corrective actions and made software patches as DEAMS was fielded to additional sites and OA2 proceeded in August 2013.

The 177th Aggressor Squadron (177 Information Assessor Squadron (IAS)) conducted a cyber-economic vulnerability assessment (CEVA) under the oversight of DOT&E. The CEVA determined that knowledgeable adversaries could penetrate DEAMS and conduct fraudulent activities; 177 IAS recommended fixes to address cybersecurity vulnerabilities.

System Description

DEAMS uses the commercial Oracle 11i solution to provide accounting and management services. It interoperates with 28 external systems that generate financial events and provide travel, payroll, disbursing, transportation, logistics, acquisition, operational, and accounting

support. The system is hosted on servers operated and maintained by the Defense Information Systems Agency (DISA) at Maxwell AFB, Gunter Annex, in Montgomery, Alabama. Users access DEAMS over the internet from their workstations via a web-enabled mission application on the Global Combat Support System – Air Force (GCSS-AF) integration framework. DEAMS equipment, operating systems, middleware, and development software conform to open systems standards and the Department of Defense (DOD) Information Technology Standards Registry. The system is compatible with the DFAS Corporate Information Infrastructure Common Operating Environment.

This page intentionally left blank.

Section Two
Test Adequacy

The IOT&E for Defense Enterprise Accounting and Management System (DEAMS) was adequate and was executed in accordance with the Test and Evaluation Master Plan (TEMP) and the detailed IOT&E plan, both of which were approved by DOT&E. Air Force Operational Test and Evaluation Center (AFOTEC) developed 40 Measures of Effectiveness (MOEs) and Measures of Suitability (MOSs) to resolve three Critical Operational Issues (COIs), nine Key Performance Parameters (KPPs), and other effectiveness and suitability parameters documented in the TEMP. The Design of Experiments (DOE), test methodology, and test measures were informed by two previous operational assessments (OAs) and continually refined among AFOTEC, the Financial Management Office (FMO), and the Program Management Office (PMO).

All testing was conducted in live environments with actual users. Because DEAMS had been in operational use for more than 5 years and the test environment was live, AFOTEC had no direct control over the sample sizes. AFOTEC mitigated this limitation by spreading the IOT&E over several months to collect necessary data determined by the DOE to a confidence level of 80 percent. The Program Executive Officer (PEO) halted testing twice to allow users to reduce transaction backlogs that were building up and causing difficulties with DEAMS usability and the operational test; these delays did not affect adequacy of testing. All cybersecurity testing was done in accordance with DOT&E policy and DOT&E-approved test plans. The Joint Interoperability Test Command (JITC) evaluated the system's interoperability with other systems and has published a separate interoperability assessment.

Test Concept

Table 2-1 depicts the relationships between DEAMS COIs, MOEs, MOSs, mission statements, and operational capabilities. The KPPs are identified with an asterisk. The grouping of capabilities with MOEs and MOSs illustrates what the users require to support the finance and accounting mission. Three COIs address DEAMS operational effectiveness and suitability:

- COI 1. Does DEAMS enable decision support? (Operational Effectiveness)
- COI 2. Does DEAMS support financial operations? (Operational Effectiveness)
- COI 3. Does DEAMS systems management support financial management operations? (Operational Suitability).

DEAMS users completed data sheets as they performed their daily tasks. The testers also collected automatic quantitative data generated by the system and employed user surveys to collect data on user experience. These data showed whether DEAMS users were able to achieve desired mission results. Some tasks were performed only by certain types of users or only at certain sites, while other tasks were universal and were performed at all sites. AFOTEC gathered data from multiple users at the various sites.

Table 2-1. Relationship of Required Capability Areas to COIs, MOEs and MOSs

COIs / Capabilities	OPERATIONAL EFFECTIVENESS Does DEAMS enable decision support?	OPERATIONAL EFFECTIVENESS Does DEAMS support financial operations?
Information Quality	MOE 1.1. Budget Resource Management MOE 1.5. Accurate balances* MOE 1.6. Budget control targets not exceeded* MOE 1.8. Reports and queries	MOE 2.2. Concurrency with standards MOE 2.3. Balance with Treasury* MOE 2.4. Accounts reconciled with General Ledger* MOE 2.5. General Ledger Operations MOE 2.7. Invalid data not entered* MOE 2.10. Accounts Payable matches MOE 2.13. Accounts Receivable (A/R) matches MOE 2.14. A/R ageing MOE 2.15. A/R liquidation MOE 2.16. Asset capitalization MOE 2.17. Asset depreciation MOE 2.19. Account closings
Timeliness	MOE 1.4. Time to record transactions	MOE 2.12. Prompt vendor payments MOE 2.18. Period-end closings*
Visibility	MOE 1.9. Ad Hoc Queries	
Usability		MOE 2.1. Role-based access control MOE 2.6. Error messages MOE 2.8. Data re-entry minimization
COI / Capabilities	**OPERATIONAL SUITABILITY Does DEAMS system management support financial management operations?**	
Interoperability	MOS 3.5. Net Ready and transfer of info*	
Reliability (Software)	Special Focus Area: Outstanding Defect Reports	
Reliability (Hardware)	MOS 3.8. MTBOMF*	
Availability	MOS 3.6. System Availability (AO) MOS 3.7. Response time during high usage	
Maintainability	MOS 3.9. Time to Restore Mission Operational Status MOS 3.10. Maintenance support MOS 3.11. System documentation	
Supportability	MOS 3.12. Help Desk support MOS 3.13. Help Desk initial response time MOS 3.14. Help Desk initial resolution MOS 3.15. Technical support documentation MOS 3.17. User documentation	
Training Quality	MOS 3.16. Rating of training	
Cybersecurity	MOS 3.1. Protection of information* MOS 3.2. Detection of intrusions* MOS 3.3. Response to incidents* MOS 3.4. Restoration of functions*	

* KPP or supports KPP

DOT&E monitored the IOT&E at the following test locations:

- Air Mobility Command (AMC): Scott Air Force Base (AFB), Illinois; MacDill AFB, Florida; Joint Base Lewis-McChord, Washington; Joint Base Charleston, South Carolina
- Air Force Global Strike Command: Barksdale AFB, Louisiana
- Air Combat Command: Tyndall AFB, Florida
- Combatant/Unified Commands: U.S. Transportation Command (USTRANSCOM) Scott AFB, Illinois; U.S. Special Operations Command and U.S. Central Command at MacDill AFB, Florida
- Help Desk Support: Wright-Patterson AFB, Ohio
- System Maintenance: Maxwell AFB-Gunter Annex, Alabama
- Defense Finance and Accounting Service (DFAS), Limestone, Maine

This page intentionally left blank.

Section Three
Operational Effectiveness

Defense Enterprise Accounting and Management System (DEAMS) was not operationally effective. DEAMS performed some mission functions well, and it supported the Air Force's financial management mission by providing a system that produced financial information in a fully electronic, and mostly automated, transaction process with an audit trail. DEAMS prevented users from exceeding budget targets and correctly computed capitalization and depreciation of assets. The system consistently reconciled subsidiary accounts to the General Ledger. However, the system did not effectively perform several critical accounting and management functions, the following four of which are Key Performance Parameters (KPPs):

- DEAMS did not provide a reliably correct balance of available funds.
- At the end of Fiscal Year (FY) 2014, DEAMS was unable to close end-of-year accounts satisfactorily. During the remaining period of the IOT&E, DEAMS did not meet the 95 percent thresholds for balancing end-of-quarter and end-of-month accounts.
- DEAMS did not record transactions in a timely manner. At one point during the test, over 3,000 travel transactions and 9,400 fuel bills were past the 24-hour timeliness threshold (some of them well past) and had not been recorded in DEAMS.
- DEAMS did not meet the 98 percent threshold for balancing funds with Treasury. DEAMS was within 0.5 percent of the threshold; however, the total dollar variance had increased by $15 Million ($15M) during the test period, indicating a possible systemic issue with maintaining proper balances with Treasury.

The results of operational effectiveness testing are discussed in the subsections that follow, arranged by general capability area. Test results for the DEAMS KPPs, including the effectiveness KPPs, are summarized in Table 3-1.

Information Quality – Decision Support

Accuracy, completeness, and timeliness of the posted data were the key indicators of successful transaction postings. DOT&E used four measures, including user surveys, to evaluate the quality of DEAMS support to budget analysts and managers who must inform senior decision-makers:

- Percentage of Balance of Available Funds reported correctly (KPP)
- Percentage of transactions automatically posted exceeding budgetary targets configured for strict funds control (KPP)
- Percentage of reports and queries generated successfully
- Operator ratings of DEAMS budgetary resource management

The test results for these information quality measures are discussed below.

Table 3-1. IOT&E Results for DEAMS Key Performance Parameters

COI	KPP	Criterion	Threshold	Attempts	Successes	Result	Confidence Interval	Assessment
COI 1. Does DEAMS enable decision support? (Operational Effectiveness)	6	MOE 1.4 Time to Record Transactions	.95 ≤ 24 hrs	112	107	.94 ≤ 24 hrs	(.92, .97)	Not met. Substantial backlogs found.
	3	MOE 1.5 Accurate Balances	≥.98	119	84	.706	(.65, .76)	Not met
	2	MOE 1.6 Budget Control Targets not Exceeded	≥.98	10,744	10,744	1.0	N/A	Met
COI 2. Does DEAMS support financial operations? (Operational Effectiveness)	1	MOE 2.3 Balance with Treasury	≥.98	1,414,442	1,379,662	.975	N/A	Not met. Total dollar variance increased.
	5	MOE 2.4 Accounts Reconciled with General Ledger	≥.95	6	6	100	N/A	Met
	4	MOE 2.7 Invalid Data not Entered	≤.02	152,393	2,974	0	(.019, .020)	Met
	7	MOE 2.18 Period-end Closings (End of Month, Quarter, Year)	.95 EOM .95 EOQ .95 EOY	44,749 38,316 4	40,621 34,801 0	.908 .908 0	(.906, .909) (.906, .910) N/A	Not met
COI 3. Does DEAMS system management support financial management operations? (Operational Suitability)	8	MOS 3.5 Net Ready and Transfer of Information	1.0	N/A	N/A	0.77	N/A	5 of 22 critical interfaces did not meet JITC NR-KPP requirements
	9	MOS 3.6 Availability (Ao)	≥.98	308 hrs uptime / 314 total hrs		.981	(.97, .99)	Met
	8	MOS 3.1 Protection of Information	See classified reports					
	8	MOS 3.2 Detection of Intrusions	See classified reports					
	8	MOS 3.3 Response to Incidents	No data					
	8	MOS 3.4 Restoration of Functions	No data					

CI = Confidence Interval
COI = Critical Operational Issue

Accurate Balance of Available Funds (KPP not met)

The accurate balance of available funds measured the degree to which DEAMS maintained fiscal accountability in balancing funds for the General Ledger and subsidiary accounts, in terms of both dollars and number of errors. The threshold requirement is 98 percent. The scope included all such transactions at the test sites. To determine accuracy for each transaction, DOT&E assessed data elements: date, organization, fiscal year, funding authority, stage of accounting, and dollar amount. The measure included individual accounting transactions, sometimes from multiple systems, that when added together equaled the total account balance. The available funds balance was considered correct if it was recorded within 10 calendar days and was numerically consistent with the original obligation.

During the IOT&E, 70.6 percent of the records examined (84 of 119) maintained accountability, with the 80 percent confidence interval ranging from 65 to 76 percent. This was an improvement over the results of OA2, in which just 60 percent (58 of 97) of the records maintained accountability, and over OA1, in which only 39 percent (23 of 59) maintained accountability. However, these results are still far short of the 98 percent threshold.

The inaccurate reports generally overstated amounts obligated and understated expensed data. The most prominent problems stemmed from paid travel orders that remained obligated. However, there were significant issues in other areas, including unpaid invoices, resulting in late charges being paid by the commands using DEAMS.

The lag time between when Treasury issued payment and the posting of those payments in DEAMS was often months. The problem was so prevalent that many users with large budgets were unable to determine how many transactions were affected. Some DEAMS reports produced large negative balances that the user was unable to explain. Experienced users were relying heavily on manual tracking of all their budgetary data on an Excel spreadsheet or in the legacy system to provide what they judged were more accurate data. Without accurate data, users were unable to use funds that were still obligated, even though those funds were in fact available. Although the users developed workarounds, they were very time-consuming, led to a high level of mistrust in the results presented by DEAMS, and fostered a reliance on legacy systems.

Budget Control Targets (KPP met)

This measure addressed the degree to which DEAMS prevented the posting of transactions that exceeded Congressional appropriation funds control targets in terms of dollars and number of errors. The threshold requirement allows a 2 percent failure rate. DOT&E assessed a system-generated log of transactions to determine: (1) whether any transactions exceeded the control targets, (2) whether any that exceeded the control targets had posted to the General Ledger, and (3) if so, whether they had an override code and user stamp. Of 10,744 transactions assessed, none that exceeded control targets were improperly posted. The measure's threshold was attained with at least 80 percent confidence.

DEAMS Reports

This measure addressed whether standard reports generated by DEAMS were timely, accurate, and complete in terms of dollars and number of errors. DEAMS did not attain the measure's threshold of 98 percent. From 184 total samples, subject matter experts considered only 102 reports (55.4 percent) to be timely, accurate, and complete.[3]

DFAS operators require a broad range of DEAMS reporting capabilities to complete their tasks. DFAS users were familiar with these reports and noted relatively few problems with the reports they use. Conversely, the base-level Air Force users use a smaller assortment of reports, but they had more problems with them. The reports most commonly run by the base-level users are the General Ledger Report, Open Document List, Travel Government Open Orders, and various program-specific and selective queries.

[3] The terms "timely, accurate, and complete" have no quantitative thresholds, but are defined in the Government Accountability Office's *Federal Information System Controls Audit Manual*. As written, (1) access to information must be punctual and reliable; (2) transactions must be properly recorded, with correct data in the proper period; and (3) transactions must be accepted for processing, processed only once and included in the output.

The most prominent reporting problem noted in IOT&E was that hundreds of travel obligations were being paid for several months after funds had been disbursed. At one time during the test, more than 2,500 travel orders that should have been closed were still open. Users implemented base-level workarounds that involved tedious manual tracking, estimating, and excluding travel data from reports. Non-travel reports fared better but still contained some errors.

Problems with DEAMS's reporting tool (Discoverer) have been noted in all previous DEAMS operational testing. To fix the problems, the PMO purchased a new reporting and ad hoc query tool known as Oracle Business Intelligence Enterprise Edition (OBIEE). OBIEE was supposed to be fielded in time for the IOT&E and is defined as part of the Initial Operating Capability, but it remained in developmental testing (DT) during the entire IOT&E period due to developmental problems and delays.

Budget Resource Management

AFOTEC employed user surveys to supplement other measures. The survey design was the same those used in the past two OAs, employing a seven-point Likert-like scale with choices of (1) completely effective, (2) moderately effective, (3) slightly effective, (4) neither effective nor ineffective, (5) slightly ineffective, (6) moderately ineffective, and (7) completely ineffective. To reach as many users as possible, AFOTEC obtained the e-mail addresses of all DEAMS users from the DEAMS Help Desk and pared them down to comprise only users at the IOT&E test sites. AFOTEC then sent e-mails to the various surveys to users at those sites according to their functional duties.

Responses from 78 users ranged from completely effective to completely ineffective, with many answering "neither effective nor ineffective." "Moderately effective" was the most popular response, but these seemingly positive results were tempered by user comments stating that they still use the legacy systems for reporting. In responding to a section on budget analysis and planning, only 52 percent (35 of 67) responded that they use DEAMS for that purpose. Hence, the survey results may not indicate user satisfaction with DEAMS capabilities, but rather with their own ability to accomplish the mission using any available method. Follow-up interviews with some users indicated the results likely correlated to the user's comfort with and continued use of legacy reporting capabilities.

User comments were informative. The general consensus was that DEAMS reporting was unreliable, cumbersome, and did not provide accurate information for decision support. Moreover, the time it took to generate a report in a readable format and drill down to specific data elements was so unsatisfactory that many users relied on other analysts to generate their data or simply revert back to the legacy Commanders' Resource Integration System (CRIS). Users were awaiting the new OBIEE reporting tool, which they hoped would give them the ability to produce DEAM reports quickly and have confidence in the information provided. However, OBIEE was not yet been operationally deployed.

Information Quality – Financial Operations

IOT&E evaluated the quality of DEAMS information support for financial operations. DEAMS must provide its users with role-based access control technology and the range of functions and data required to complete financial mission tasks.

Standards Concurrency

IOT&E evaluated the extent to which the system complied with Standard Financial Information Structure (SFIS) business rules. These business rules encompass a common business language that enable budgeting, performance-based management, and financial statement generation. SFIS is a comprehensive data structure that supports requirements for budgeting, financial accounting, cost/performance, and external reporting needs across the Department of Defense (DOD) enterprise. The SFIS compliance checklist contained 319 items. DOT&E evaluated all 319 items and found that they were all compliant. The threshold was 95 percent. DEAMS concurs with the applicable business standards.

Balance with Treasury (KPP not met – Close to threshold)

DEAMS nearly met the 98 percent threshold for balancing funds with Treasury but the total dollar variance increased by nearly $15M during the test period. The measure addressed whether DEAMS funds balanced with Treasury account balances at the accounting fund level. The Fund Balance with Treasury calculation reflects available budget spending authority on a monthly basis. DOT&E used the February 2015 and April 2015 end-of-month Consolidated Cash Accountability System reports to measure Fund Balance with Treasury, calculating that 1,379,662 of 1,414,442 fund account balances (point estimate of 97.5 percent versus a 98 percent requirement) matched the Treasury fund account balances. Because of the large sample size, the 80 percent confidence interval is essentially equal to this point estimate.

The unmatched lines of accounting increased steadily beginning with the September 2014 software update before IOT&E began and reached a peak in October 2014, indicating that there may have been systemic issues with maintaining proper balances with Treasury. The increase in unmatched lines coincided with the deployment of DEAMS to additional Air Force Bases (AFBs). From October 2014 to April 2015, the total dollar value variance increased by 11 percent, from $135.8M to $150.7M, as older backlogged items continued to grow. If the current trend continues, there will be more strain on DFAS manning and achieving auditability will become increasingly difficult. The three main causes for the imbalance (of which one was fixed and two that could not be resolved during the IOT&E) were:

- A problem with the Departmental Cash Management System (DCMS) interface following the partial deployment of Release 3 has been fixed with a code patch.
- A significant increase in the number of Transactions by Others that were not reflecting in DEAMS.
- Pre-existing backlogged transactions were not cleared in a timely manner (i.e., within days rather than weeks or months). The upcoming increase in DEAMS users from 5,000 to 29,000 will likely exacerbate the current backlog and increase the number of

unmatched lines without significant changes to the transaction processing or increases in technicians to fix erroneous transactions.

Reconciliation with General Ledger (KPP met)

This measure addressed whether subsidiary accounts were reconciled to General Ledger control accounts in terms of dollars and number of errors. A General Ledger control account is any account listed in the United States Standard General Ledger Chart of Accounts. Subsidiary accounts are successfully reconciled when all differences are identified, accountability for those outstanding variances is assigned, and the differences explained. DFAS performs a complete reconciliation between DEAMS General Ledger control accounts and subsidiary accounts once a week. The test team reported that DFAS successfully reconciled all six modules (100 percent) comprising 85 accounts on a weekly basis.

General Ledger Operations

This measure addressed DFAS success in balancing funds in DEAMS using U.S. Treasury tie-point analysis guidelines. Testing covered both General Funds and Working Capital Funds and considered both the number of funds examined and the absolute dollar value of any that were out of balance. DFAS and the FMO use a locally developed tool for tie-point analyses that utilizes standard U.S. General Ledger accounting relationships to determine out-of-balance conditions.[4] DOT&E measured the 52 tie point balance reconciliations within DEAMS and found two imbalances. Therefore, 96 percent of the tie-points were balanced, exceeding the requirement of 95 percent. The 80 percent confidence interval ranged from 90.2 percent to 97.9 percent.

Rejection of Invalid Data (KPP met)

IOT&E measured instances where DEAMS allowed processing of invalid data that corrupted the database or were not in compliance with financial regulations (DOD Core Financial System Requirements). The threshold allowed a margin of 5 percent corrupt or invalid data, graded in terms of both dollars and number of errors against a monthly set of transactions. The DEAMS program self-reports this metric. For the month of April 2015, 2,974 of 152,393 transactions (2 percent) were reported as invalid, which met the threshold with 80 percent confidence.

Accounts Payable and Accounts Receivable

The Accounts Payable Matches measure addressed the degree to which DEAMS matched Accounts Payable documents to appropriate source document line items in terms of the number of late payment errors and the amount of time by which late payments exceeded timelines. The threshold allowed a 5 percent failure rate. The test team collected 1,818 samples and none had matching errors. This measure met the threshold with 80 percent confidence.

[4] "Tie-points" are relationships between standard General Ledger accounts. Tie-point analysis was developed by the Department of the Treasury to assist agencies in reconciling and balancing accounting information in U.S. Standard General Ledger format.

The Accounts Receivable Matches measure addressed DEAMS precision and thoroughness in matching and applying Accounts Receivable collections to Accounts Receivable balances to determine whether payments were posted against the account correctly. DOT&E compared observations with a system-generated report covering all Accounts Receivable collections occurring during the test period in both the general fund and working capital fund. Of 1,632 transactions, 82 (5.0 percent) had errors, which met the threshold. The 80 percent confidence interval ranged from 94.2 percent to 95.6 percent.

Accounts Receivable Ageing and Liquidation

The Accounts Receivable Ageing measure addressed the degree to which DEAMS correctly computed and aged Accounts Receivable transactions in terms of dollars and number of errors. The minimum threshold was 90 percent and this was attained with 80 percent confidence, with 50 of 50 samples (100 percent) aged successfully.

The Accounts Receivable Liquidation measure addressed the degree to which DEAMS correctly accomplished Accounts Receivable liquidation transactions in terms of both dollars and number of errors. The threshold allowed a 5 percent liquidation error rate and none were found in 3,106 transactions. The threshold was attained with 80 percent confidence.

Asset Capitalization and Depreciation

The Asset Capitalization measure addressed the degree to which DEAMS successfully capitalized assets and tracked them based on their pre-identified capitalization thresholds. In accounting, "capitalization" refers to determining the true cost to acquire a new asset when all expenses are considered. DOT&E selected a sample of 133 assets. All 133 line items were successfully capitalized in DEAMS resulting in a 100 percent success rate, achieving the 95 percent threshold with 80 percent confidence.

The Asset Depreciation measure addressed the degree to which DEAMS successfully depreciated assets. To verify successful depreciation of assets, the test team examined DEAMS Fixed Assets Cost Reports at Headquarters USTRANSCOM and Headquarters AMC. DOT&E found that 168 of the examined 168 assets (100 percent) were depreciated successfully, meeting the measure's 95 percent threshold with 80 percent confidence.

Account Closings

This measure addressed whether DEAMS successfully completed all necessary actions relating to the closing of year-end accounting periods. Year-end closing is closely related to a separate measure, "Period-End Closings," also a KPP. The two measures are discussed separately in this report because "Account Closing" is an information quality issue, while the KPP "Period-End Closings" is a timeliness issue. Neither issue met threshold requirements.

The "Account Closing" measure applied to month-end and year-end account closures. DEAMS derived an accounting period's closing balances at the United States standard General Ledger attribute level. For a successful closing, DEAMS had to perform the procedures according to the prescribed requirements and the actual close date had to match the expected accounting period close date. For each closure, DOT&E verified whether DEAMS was able to

do the closing, or whether user intervention was required. DOT&E used the Treasurer Financial Manual to evaluate accuracy. The test team observed the 2014 Fiscal Year-End (FYE) closeout in October 2014 and the end-of-month closeout for January 2015. The end-of-month closure performed as expected but the FYE closeouts did not occur within requirements or on the anticipated accounting period close date at the Air Force level or at the four operational bases the team visited.

Various types of transactions failed, causing the PEO to temporarily halt DEAMS processing of these transactions. Backlogs began to develop and the PEO decided to suspend IOT&E until the backlogs and software deficiencies could be resolved. During the closeout itself, a General Ledger stopped updating, final account balances could not be validated, an Open Document List was inaccurate, a Status of Funds could not be pulled in a timely manner, transaction statuses could not be confirmed, and a selective transaction history was unavailable to back up the Status of Funds. Some DEAMS users characterized the 2014 FYE closeout as the worst FYE closeout they had ever witnessed.

Timeliness

The measures discussed in the subsections that follow evaluate the operational effectiveness attribute of timeliness, which is vital to both decision support and financial operations. Transactions must be recorded quickly to be relevant and to ensure prompt payments to vendors. Month-end and year-end closings must be done within strict time constraints to support the next financial accounting period.

Period-End Closings (KPP not met)

This KPP measure evaluated DEAMS ability to provide financial information to users after specified accounting periods (monthly, quarterly, and yearly) have been formally closed by decision-makers and locked down by the system functionality. An account was successfully closed when the data were available to the official financial reporting system by the prescribed date. The threshold for each period was 95 percent. The point estimate results and confidence intervals for each period were:

- Monthly. From October 2014 through April 2015, 40,621 of 44,749 accounts (90.8 percent) successfully closed by the prescribed date. The 80 percent confidence interval ranged from 90.6 to 90.9 percent.
- Quarterly. During the first quarter of FY15 (1QFY15), 16,559 of 18,465 accounts (89.7 percent) successfully closed by the prescribed date. During the 2QFY15, 18,242 of 19,851 accounts (91.9 percent) successfully closed by the prescribed date. For the two quarters, 34,801 of 38,316 accounts (90.8 percent) successfully closed by the prescribed date. The 80 percent confidence interval ranged from 90.6 to 91.0 percent.
- Yearly. No accounts were successfully closed by the prescribed date at the four bases that the team visited in October 2014.

The failure of DEAMS to support a successful FYE closeout resulted in an increased workload, inability to execute excess funds, and loss of confidence in the system. Users reported a greater number of Help Desk inquiries, longer problem resolution times, and a lack of information dissemination. Many users recalled that DEAMS began to experience increased problems after the FYE software patch. The problems caused by this patch are discussed later in this report, in the Operational Suitability section, under Configuration Management and Regression Testing.

Time to Record Transactions

This measure addressed the time required to record commitment and obligation transactions. Data were collected randomly from system logs to calculate the time between certification of an operator transaction and when the transaction posted to the DEAMS General Ledger. The time was faster than the 24-hour maximum requirement in 105 of 112 samples (94 percent). The measure's 95 percent threshold was not attained; although the point estimate of 94 percent is quite close to the threshold, many transactions far exceeded the threshold leading DOT&E to conclude that this measure was not met and had a meaningful impact on financial operations and user workload.

Although not found in the sampled test event, many more transactions from other systems (such as the Defense Travel System) failed to post in DEAMS within the 24-hour threshold during the period of the IOT&E. The test team reported a backlog of transactions that had entered DEAMS from an interface stuck in an error status. The backlog contained transactions from every month during the period October 2014 through May 2015, resulting in financial status report inaccuracies. Transactions from previous fiscal years were also found in the error table. DFAS was unable to clear the transaction backlog in a timely manner (i.e., within days rather than weeks or months). For example, there were over 11,000 items more than 120 days old that the test team identified when testing restarted the week of May 18, 2015. DOT&E identified 146 of 793 paid orders at one Air Force Reserve Wing that were paid but not recorded with several hundred more pending research. As previously noted, deployment of DEAMS to additional users will likely exacerbate the transaction backlog issue.

Prompt Vendor Payments

This measure addressed the degree to which DEAMS made payments to vendors within timelines specified in the Prompt Payment Final Rule in terms of both dollars and number of errors.[5] Of 11,662 vendor payments, 10,451 (89.6 percent) were within specified timelines. The measure did not meet the 95 percent threshold.

There was a large increase in late vendor payments from October to January, as shown in Figure 3-1. The spike remained above the AF Goal through April 2015. The root cause was a backlog that began with temporarily halting transactions in October and November 2014. The

[5] The Prompt Payment Final Rule is in Office of Management and Budget (OMB) Circular A-125 and has been codified (5 CFR 1315). It defines the timelines required to realize vendor discounts and avoid late payment penalties.

increase in penalty payments to $465.74 per $1M in January 2015 was nearly 10 times the Air Force's FY15 goal of $49.00 per $1 million before dropping to $90.00 per $1M by April.

The PEO halted the IOT&E twice, for a total of 5 months, to allow time for the PMO and DFAS to clear backlogged transactions. As reflected in Figure 3-1, metrics gathered after the pause showed a marked improvement in vendor payment promptness by April 2015, which is the last month reported, but the payments continue to exceed the Air Force's 2015 goal. It is unknown whether this event was an aberration or whether there are other underlying issues, such as defective software, process change, volume, or some combination of these. Equally uncertain is how adding more DEAMS bases will affect future backlogs; however, the trend is moving rapidly towards meeting the end goal. This should be assessed in future OT&E.

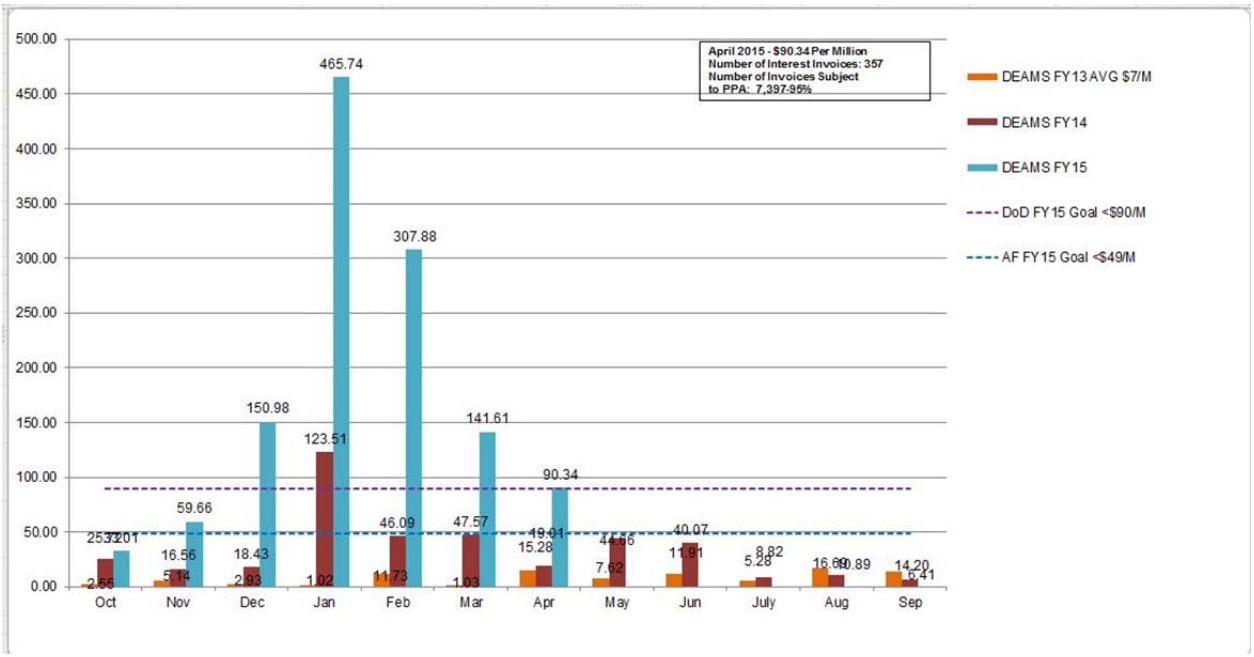


Figure 3-1. Late Vendor Payments during the DEAMS IOT&E

Visibility

Ad Hoc Queries

This measure addressed the capability of DEAMS ad hoc queries to provide financial information to the user and included evaluating content, format, and applicability of ad hoc queries. An ad hoc query is defined as a report designed specifically to provide the information necessary for certain financial operations.

When the test plan was written, it was expected that the new OBIEE reporting tool would have replaced Oracle Discoverer by the time of the IOT&E, but it had not. Thus, the survey results from the IOT&E were very similar to those obtained during OA2 with "moderately effective" being the most common response. User comments indicated widespread dissatisfaction with the Discoverer tool.

As with user surveys previously discussed under the measure titled "Budget Resource Management – User," DOT&E used a seven-point Likert-like scale. While survey results, shown in Figure 3-2, present an overall positive result, user interviews indicated that the results likely correlated with the user's comfort with and continued use of legacy reporting capabilities. The interviewers concluded that the high scores actually reflected user satisfaction with the reports they were able to piece together from the legacy systems. For this figure and similar graphics throughout this report, the "Y" axis denotes numbers of responses.

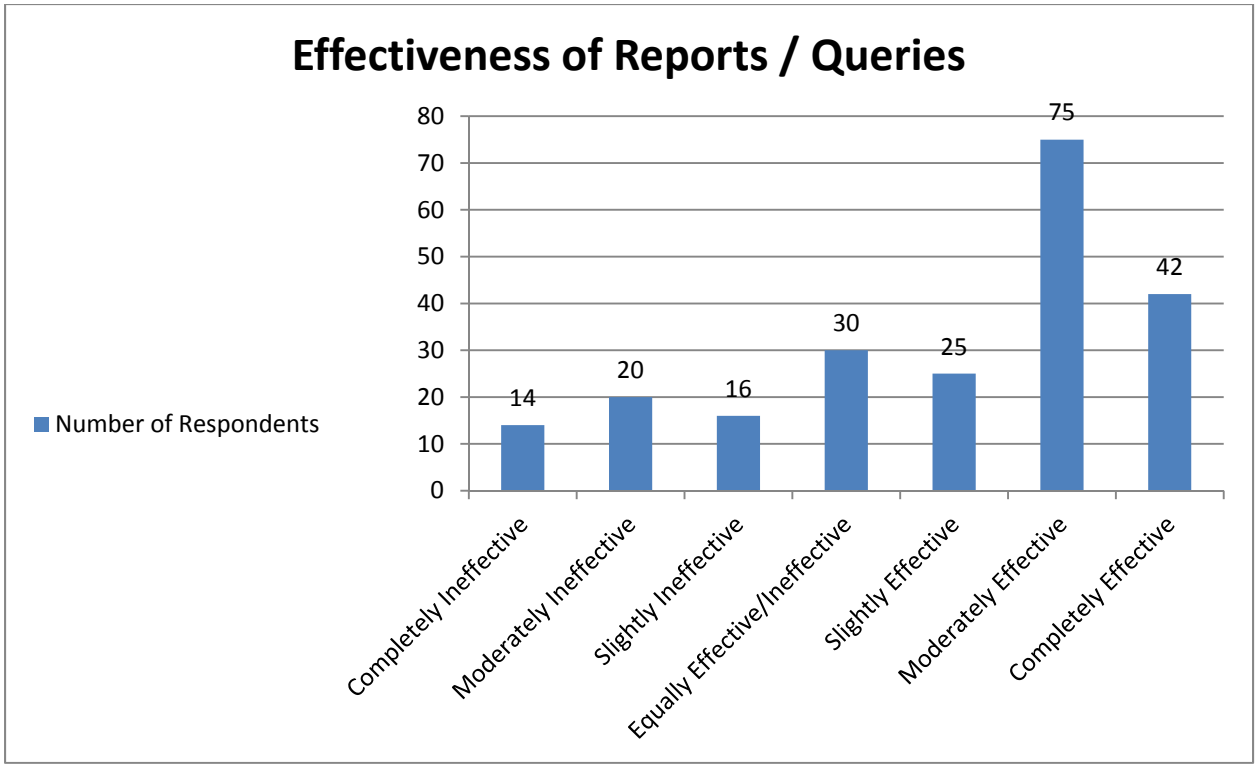


Figure 3-2. User Opinions of Reports and Queries (using either legacy systems or DEAMS)

The primary respondent complaints regarding DEAMS included difficulty in finding the correct report to run, the time the reports take to run, and the perception that the Discoverer standard reports simply did not meet their needs. They noted that the reports were hard to understand, not clearly presented, contained too little or too much information, and were not customizable.

Usability

The Usability measures addressed the ease with which users could employ DEAMS to provide decision support or manage financial operations. Usability examined access controls, data entry, and error messages. Users were assigned access appropriate to their roles and the required accesses and data reentry were not problematic. The quality of automatic error messages was inadequate, requiring users to involve the Help Desk to understand and resolve issues.

Role-Based Access Control

IOT&E measured whether users were assigned the access appropriate to their role and the degree to which they were able to do their jobs within the role access they were assigned. This was done by determining the percent of assigned operator roles that were compliant with the document *Comptroller Access Guide, Segregation of Duties, Policies, and Procedures.* DOT&E reviewed the roles and responsibilities of all DEAMS users. There were 15 (of 5,524) users with 41 (of 48,280) conflicting roles. All conflicting roles had current waivers. DEAMS was 100 percent compliant with *Comptroller Access Guide* role-based access control guidelines.

Data Reentry Minimization

This measure addressed the capability of DEAMS to support single data entry. Information should enter the system once from the appropriate source and be immediately available. Once accounting data pass edit checks and enter the system database by either interfacing with another system or through manual input, no further entry of the same data should be required to complete the business event.

DOT&E evaluated a sample of standard transactions for instances of data re-entry employing a daily, user-maintained log that identified the numbers and kinds of entries, noting any that required duplicate entries. The threshold required 5 percent or less of transactions to have reentry of transaction data, and DEAMS achieved this rate with only 4 of 116 recorded transactions (3.4 percent) requiring reentry.

Effectiveness of Error Messages

User surveys rated the effectiveness of DEAMS error messages with respect to accuracy, clarity, scope, traceability, and resolution aid. These results were consistent with the results from previous operational assessments. Users continued to express frustration with the lack of clarity in the error messages and with having to restart or reenter their work rather than just fixing the error and continuing the transaction. Users complained that the error messages were in technical, rather than user-understandable financial terms, and that often no course of action was obvious from the error message. The PMO prepared a cross-walk document to aid users in decoding Oracle error messages, but very few users at the test sites had the document available. Providing technical aids addressing known error messages with practical actions to resolve the issues for the users will help to mitigate the problem.

Section Four
Operational Suitability

DEAMS is not operationally suitable and is not ready for sustainment. The system met its reliability, availability, and maintainability hardware measures, attaining the operational availability (A_o) threshold of 98 percent. However, five critical interfaces did not work properly and DEAMS exhibited software reliability growth as measured by the increase in the amount of deficiencies during the IOT&E, including many high severity deficiencies that have remained unresolved for 240 days or longer.

- More high severity Incident Reports were extant at end of test (81) than when the test began (33).
- The DEAMS Functional Management Office (FMO) reported 65 outstanding Severity-2 defects at end of test. There were 20 of these that were more than 240 days old.
- The FMO reported 50 outstanding Severity-2 Software Change Requests at end of test. There were 35 of these that were more than 240 days old.
- As of May 27, 2015, 15 incident reports rated as Severity-2 were more than 2 years old.

Measures of operational suitability were used to assess A_o, hardware reliability, maintainability, supportability, interoperability, training quality, and cybersecurity. The results of operational suitability testing are discussed below, arranged by general capability area. This section also discusses suitability areas of special interest for which there were no specific test events or quantitative measures. These areas include software reliability, configuration management, and regression testing. Test results for the DEAMS Key Performance Parameters (KPPs), including suitability KPPs, are summarized in Table 1 (in the Executive Summary).

Reliability and Availability

RAM was evaluated over the 7-month period from October 1, 2014, through April 30, 2015, using the operational time frames of 5:00 a.m. to 5:00 p.m. Monday through Friday and 6 a.m. to 12:00 p.m. on non-patching Saturdays, for 2,002 record test hours. Because accurate system downtime data were only available for the month of April 2015, A_o was computed using April data only.

Operational Availability (A_o) (KPP met)

This measure determined the A_o of DEAMS servers and interfaces at the Defense Information Systems Agency (DISA) Defense Enterprise Computing Center at Maxwell-Gunter Annex, Alabama. A_o was determined by dividing the uptime (total time minus 6 hours of unscheduled downtime) of 308 hours by the total time (314 hours) measured during the month of April 2015, the last month for which data were available. The calculated A_o was 98.1 percent with the 80 percent confidence interval ranging from 97 to 99 percent. The threshold is 98 percent, hence DOT&E cannot state with confidence that the requirement is met. Scheduled

downtime was not a factor because it took place during periods that DEAMS was not scheduled to operate.

DEAMS is not yet supporting worldwide operations, so it's operational time is not a full 24 hours per day. This allows for a wide window for preventive maintenance, or even unscheduled repairs that occur outside of the operational hours, without affecting operational availability. DEAMS will ultimately deploy to overseas locations, so the non-operational window will be narrowed or perhaps eliminated. In preparation for these deployments and subsequent near-constant mission status, the PMO should prepare preventive maintenance plans to minimize scheduled downtimes. In addition, site failover plans to the backup site should continue to be developed and refined to ensure continued mission support in the event of an unscheduled extended failure during mission hours.

Hardware Reliability

This measure determined the Mean Time between Operational Mission Failure (MTBOMF). DEAMS experienced eight hardware failures during the 2,002-hour test period, resulting in a point estimate of 250 hours MTBOMF with 80 percent confidence bounds of 154 and 430 hours. This met the hardware reliability threshold of 96 hours with 80 percent confidence.

Maintainability and Supportability

This group of eight measures evaluates maintainability and supportability and related documentation issues at the DEAMS and DISA Help Desks, maintainer locations, and at the alternate DEAMS site in Utah. The DEAMS Help Desk provided timely, effective support at the first tier. Users were more critical of the support they received for problems referred to higher tiers that had not been resolved as quickly. The DISA Help Desk provided technical support to the system in the Global Combat Support System – Air Force (GCSS-AF) environment. Both DEAMS system maintainers and DISA technical maintainers rated the documentation highly.

Time to Restore Mission Operational Status

This measure determined the time to restore mission operational status following a failure. In December 2013 and January 2014, during OA2, the FMO conducted continuity of operations testing on four occasions in preproduction environments at Maxwell-Gunter Annex, Alabama, and Hill Air Force Base, Utah (the backup site). Execution of the complete failover phase averaged 2.1 hours over the four events with the shortest time being 1.5 hours and the longest time being 4 hours, thus attaining the 6-hour threshold in each case. Additional failover testing was not conducted for the IOT&E.

Maintenance Support

To assess this measure, all available DEAMS system maintainers at Maxwell-Gunter Annex were asked to rate "ease of maintenance" across six areas: (1) system start-up, (2) shutdown, (3) monitoring, (4) recovery and restart, (5) internal processing controls, and (6) archiving and application security. Five maintainers completed the survey and all of them responded that start-up, shutdown, and archiving were "completely effective." All five

respondents also rated the other three areas in the "effective" categories. The maintenance support surveys showed improvement over both operational assessments (OAs).

System Documentation

This measure addressed the installation and maintenance documentation at Maxwell-Gunter Annex for procedures governing configuration and system sustainment of hardware and software in accordance with the Federal Information System Control Audit Manual. The testers rated all 16 checklist items applying to DEAMS as compliant.

Technical Support Documentation

To assess this measure, all available DISA system maintainers at Maxwell-Gunter Annex were asked to rate the adequacy of technical documentation with respect to (1) sufficiency of scope/coverage, (2) accuracy, (3) clarity, (4) actionability (sufficient direction), and (5) accessibility. Of the seven Help Desk personnel who responded, six rated technical documentation as either "completely effective" or "moderately effective." The one maintainer who rated the documentation ineffective felt that the aids were geared to a general overview and did not reflect the actual scenarios that might be experienced. This maintainer stated that it could be difficult to find the right guide to send to a particular user and that the guides needed to be tied together to better document the entire process.

Help Desk Support

All available users were asked to rate the adequacy of DEAMS Help Desk support by completing a seven-point rating scale questionnaire. Users also provided comments to identify specific strengths and critical problems. There were 168 respondents, of which 113 (67 percent) rated the Help Desk effective, which was below the 85 percent point estimate threshold. There were 27 users (16 percent) who rated the Help Desk ineffective and 28 (17 percent) chose to answer "neither effective nor ineffective." These results were less positive than the results from OA2, in which 137 of 161 respondents (85 percent) had rated the DEAMS Help Desk as effective, meeting the threshold.

As with prior surveys, the satisfied users were often those who had simpler problems that could be solved at the first level. The unsatisfied users complained of the lack of financial management expertise at the Level 1 Help Desk. They noted that the Help Desk sometimes did not understand their specific problems and did not ask for further information or clarification. They noted that they were not informed when their issue was resolved and that many of their issues had not been resolved. DOT&E expressed concern in our report on OA2 that the need for more Help Desk personnel familiar with DEAMS financial processes as well as legacy systems could become a problem as more bases acquired DEAMS. The survey results may reflect this. If so, the problem will be exacerbated as the number of DEAMS users increase in the months to come.

Figure 4-1 shows the spread of responses to the Help Desk questionnaire by number of respondents at each level, with a median response of "moderately effective."

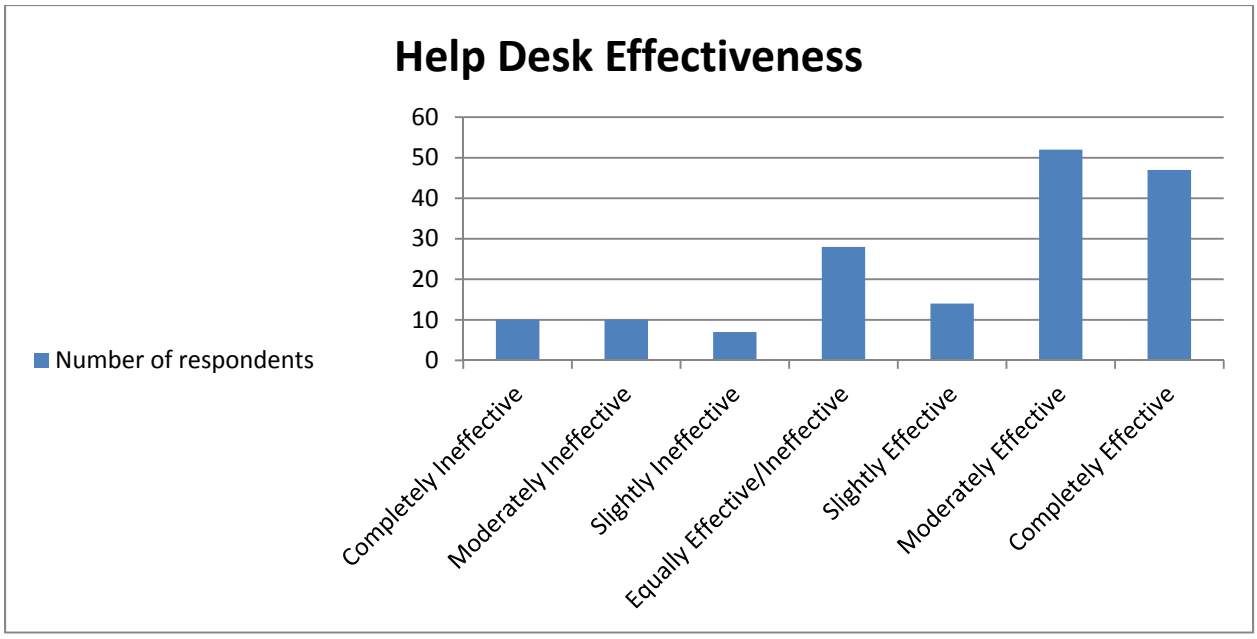


Figure 4-1. User Opinions of the DEAMS Help Desk

Help Desk Initial Response Time

This measure used DEAMS Help Desk logs to measure the time required to provide initial assistance during duty hours. The measure focused on the time it took Help Desk personnel to provide initial assistance and did not include final resolution of the problem. Users contacted the Help Desk 1,539 times from April 4 through 30, 2015. The maximum response time was 22 hours, while the minimum was 1 minute. The threshold was for all responses to be made in no more than 4 hours.

For phone contacts, 100 percent of calls were answered on the first attempt. The overall average response time for all 1,043 emails was 1.55 hours with a standard deviation of 2.2 hours. The preponderance of email responses (980 of 1,043, or 94 percent) were under the 4-hour threshold. The Help Desk responded to 96 percent of all contacts within 4 hours, with 63 email responses taking longer than 4 hours, which was not considered an operationally significant shortfall.

Help Desk Resolution on First Attempt

This measure addressed the proportion of Help Desk initial incident resolutions that were resolved on the first attempt. There were a total of 1,937 calls and emails from operational users during the test period (April 4 through 30, 2015).[6] Of these, 1,844 (95.2 percent) were resolved on the first attempt, meeting the threshold of 95 percent. The DEAMS Help Desk, however, resolves only basic problems. Sometimes "initial resolution" consists of opening a trouble ticket and referring the problem to a higher tier. As noted in the Help Desk Support surveys, some

[6] This number is higher than the number of contacts cited in the previous measure because about 200 trouble tickets did not contain the times needed for the previous measure and were excluded. Many of the tickets that contained no times appeared to have been resolved very quickly.

users expressed frustration at the lack of financial management expertise at the Level 1 Help Desk.

Regression Testing

The program became schedule driven in order to support and evaluate the Fiscal-Year-End (FYE) account closing functionality and was pressed by the scheduled IOT&E, which began on October 1, 2014. Consequently, the DEAMS program fielded part of Release 3.2 without including regression testing by the Lead Developmental Test and Evaluation Organization in the Capabilities Integration Environment and by the 46th Test Squadron in the GCSS-AF pre-production environment before placing new software in the production environment.

The new software failed to perform the FYE closings satisfactorily. In addition, introduction of Release 3.2 into the live environment without properly performing regression testing may have affected the fielded DEAMS software. Other types of transactions began to fail, causing the Program Executive Officer (PEO) to halt DEAMS processing of these transactions temporarily. Substantial backlogs began to develop and the PEO decided to suspend IOT&E until the backlogs and software deficiencies could be resolved. The IOT&E did not resume until February 17, 2015. However, backlogs were still adversely affecting both DEAMS usability and the IOT&E, so the PEO suspended testing for another month. The presence of backlogs and software defects sufficient to interrupt the IOT&E strongly indicated that DEAMS is neither operationally effective nor operationally suitable. The IOT&E officially ended on May 29, 2015, with backlogs still present.

Software Reliability – Outstanding Defects

For information systems, software reliability is reflected by the number of outstanding defects and the trend of these numbers over time. The DEAMS incident reporting system uses the *Serena Business Manager*® trouble ticketing program. *Serena* can track trouble tickets opened by the Help Desk and escalate tickets to Deficiency Report or software change request (SCR) status should the Help Desk be unable to resolve the issue. Approximately 67 percent of all Help Desk tickets are resolved during the initial call, about the same as the 68 percent first-call resolution rate average of the call-center industry.

DEAMS software reliability growth planning is focused first on resolving incidents reported to the Help Desk as soon as possible, if they are amenable to quick resolution. Systemic problems requiring changes to the software are reviewed by a monthly review board that determines the severity level (1, 2, 3, or 4) of the issue and whether the resolution requires a Deficiency Report or an SCR.[7] The System Integrator is required to fix Deficiency Reports as part of the existing contractual agreement, whereas the government must pay for software patches that resolve SCRs, which are changes to requirements previously negotiated.

Figure 4-2 shows the cumulative open defects over a six-month period during the IOT&E. DEAMS had 151 total open defects at the end of December 2014 and 201 when the

[7] The definitions of severity levels for DEAMS Deficiency Reports and SCRs are aligned with those contained in IEEE Standard 12207.2, Annex J, dated April 1998.

IOT&E ended in May 2015, an overall increase of 33 percent. This compares with an overall *decrease* of 9 percent (from 111 to 91) observed during OA2. DEAMS ended the IOT&E with more than twice as many defects extant in January 2014 at the end of OA2. No Severity 1 defects were noted during the IOT&E, but Severity 2 defects (represented by blue bars) steadily climbed from 41 in December to 65 in May, a rise of nearly 60 percent. During OA2, Severity 2 defects had decreased from 30 through December 2013 to only 17 in January 2014. These numbers do not include Incident Reports that were awaiting adjudication. More Incident Reports were extant at end of test (81) than when the test began (33). These trouble tickets usually begin as Severity 3 incidents by default, until the severity level is assigned by a review board. It is highly likely that some of the incident reports will be reclassified as Severity 2 by the review board.

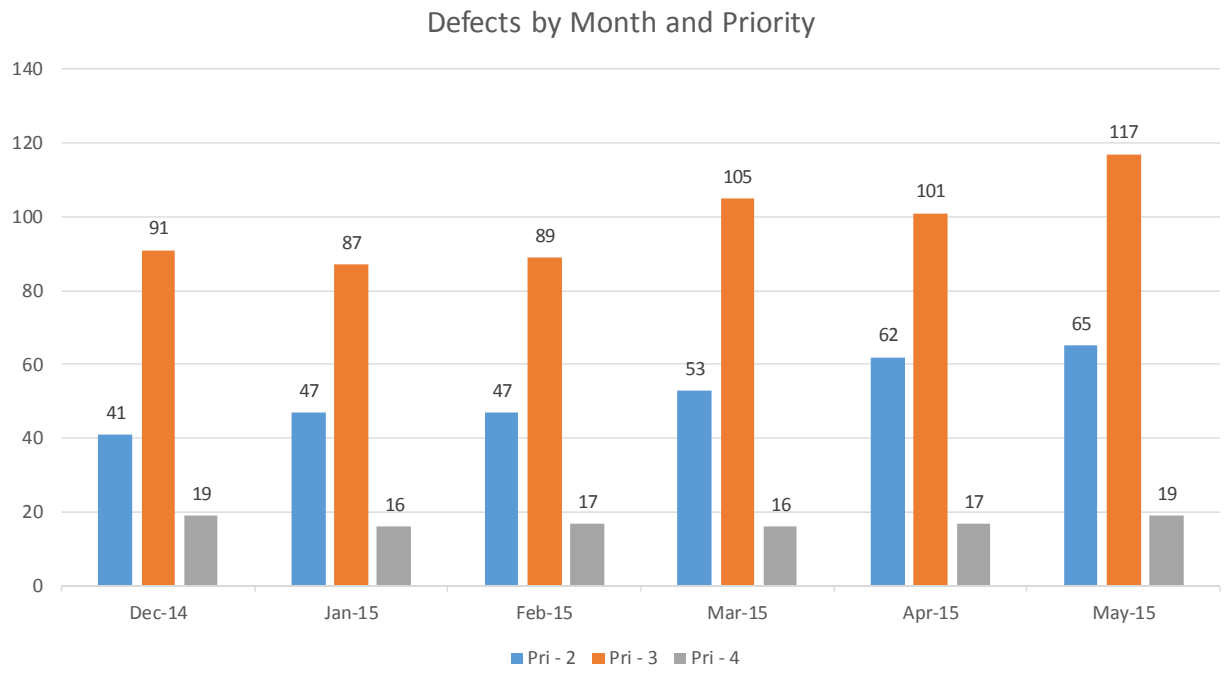


Figure 4-2. Cumulative Open DEAMS Deficiency Reports by Month and Severity during the IOT&E

Thus, DEAMS exhibited software reliability growth as measured by the increase in the amount of deficiencies during the IOT&E including many high severity deficiencies that have remained unresolved for 240 days or longer. This is illustrated in Figure 4-3, which shows the aging of open defects as of May 31, 2015. Of the 65 Severity 2 defects present at end of test, 20 (more than 30 percent) were more than 240 days old which is before the start of the IOT&E.

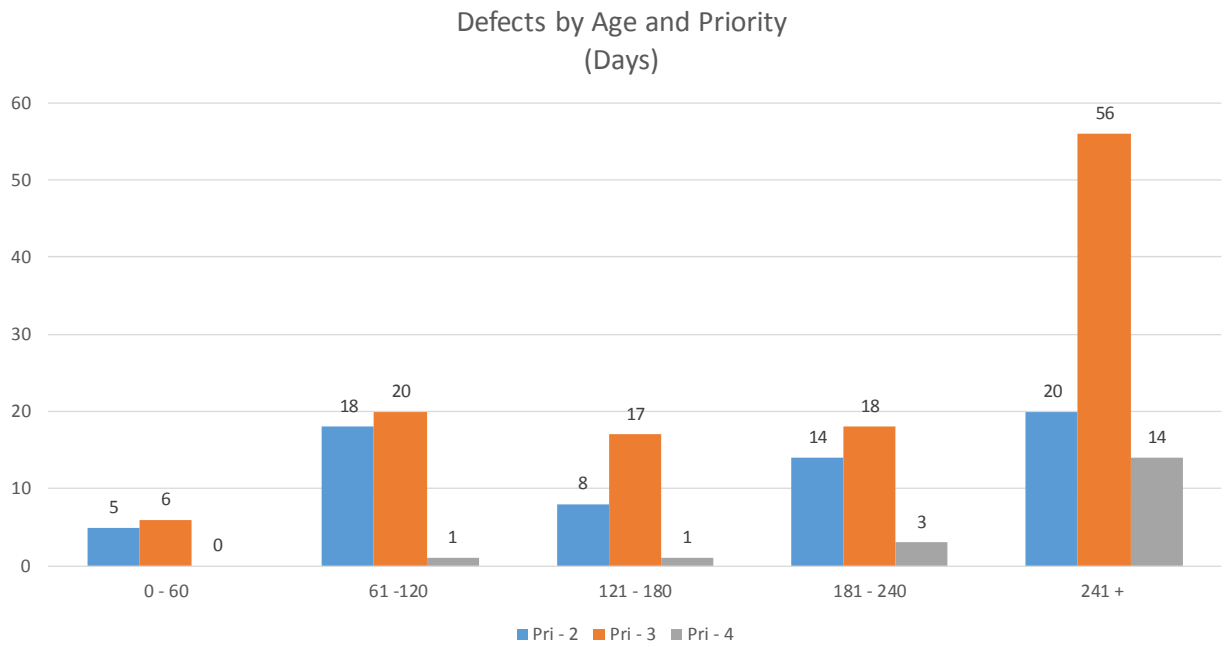


Figure 4-3. Age of DEAMS Deficiency Reports as of May 31, 2015

The trend is also evident with SCRs, as illustrated in Figure 4-4. DEAMs had 227 total open SCRs at the end of December 2014 (light blue bars) and 259 when the IOT&E ended in May 2015 (green bars), an overall increase of 14 percent. A significant number of these SCRs are greater than 240 days which is before the start of the IOT&E.

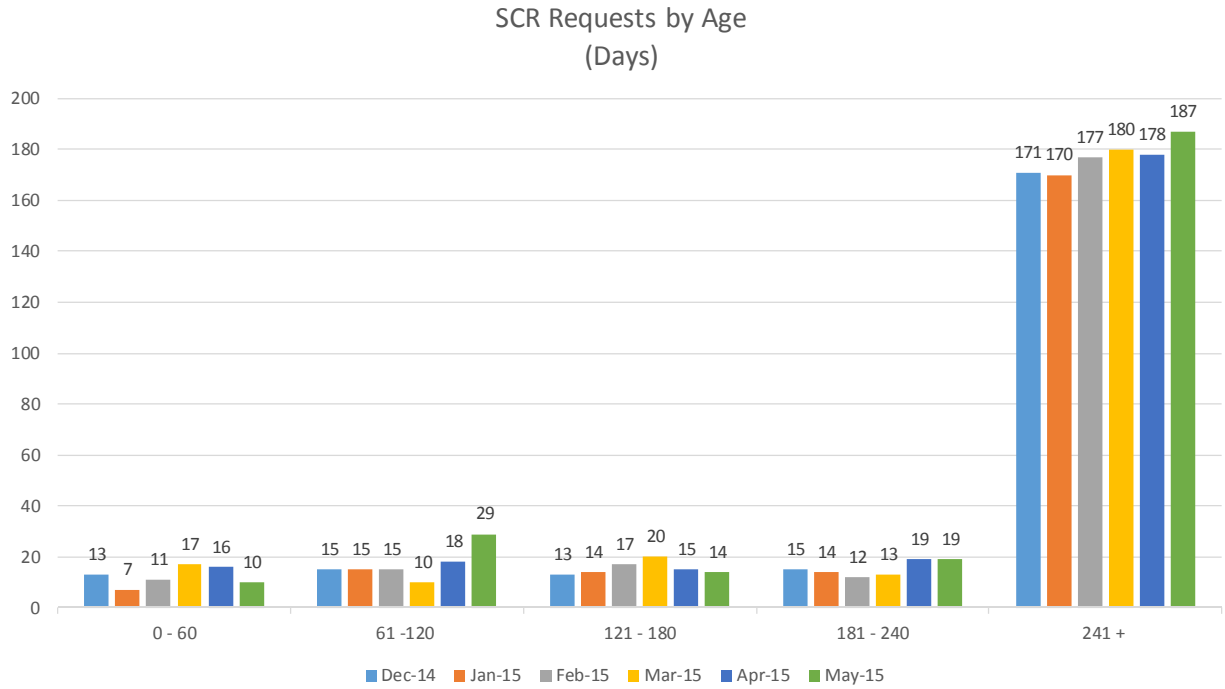


Figure 4-4. Age of DEAMS System Change Requests by Month and Severity during the IOT&E

Figure 4-5 focuses on the aging of open SCRs as of May 31, 2015. Of the 50 Severity 2 SCRs present at end of test (blue bars), 35 (70 percent) were more than 240 days old. Of the 163 Severity 3 SCRs present at end of test (orange bars), 118 (72 percent) were more than 240 days old.

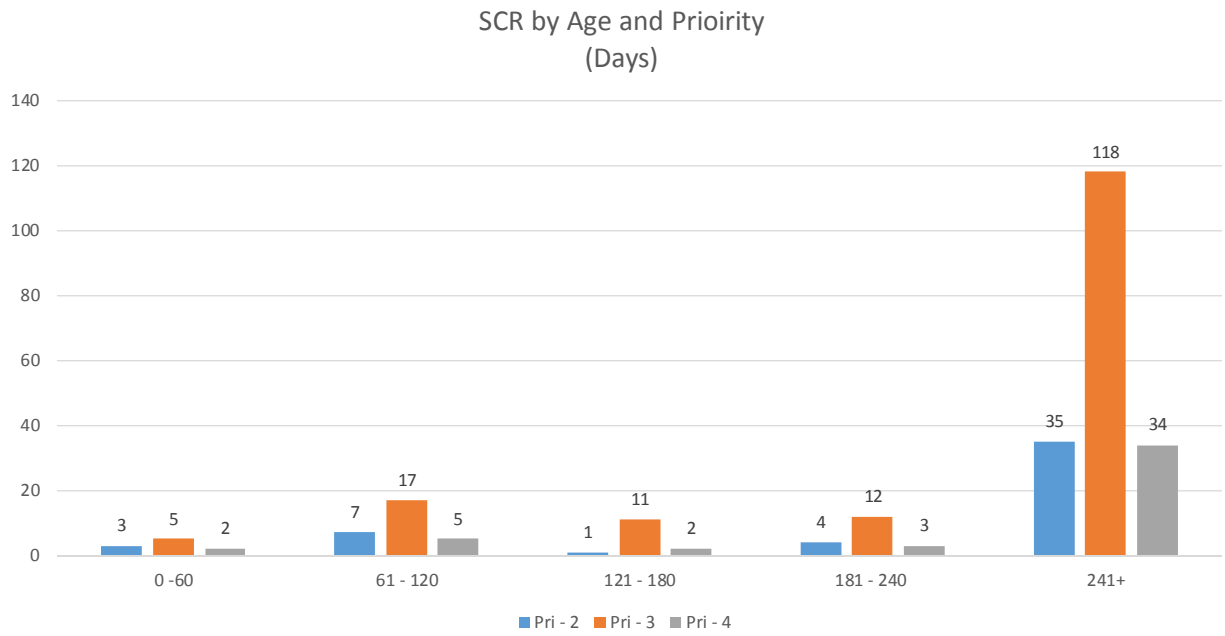


Figure 4-5. Age of DEAMS System Change Requests as of May 31, 2015

Interoperability

Net Readiness (KPP not met)

The Net-Ready KPP assesses whether DEAMS is able to exchange data via the interfaces described in the DEAMS System View-6 Systems Data Exchange Matrix. DEAMS currently has 59 external joint interfaces, 23 of which are designated "mission critical." The Joint Interoperability Test Command (JITC) conducted an Interoperability Assessment of the DEAMS based on the data from August 2014 through May 2015. JITC collected data and assessed DEAMS in the GCSS-AF production environment located at Maxwell Air Force Base (AFB) – Gunter Annex, Montgomery, Alabama. The results of the assessment demonstrated that 5 of the 22 available critical interfaces did not meet the required information exchange requirements. JITC assessed 46 of the 59 external interfaces (22 critical and 24 non-critical). JITC did not assess 13 of the 59 external interfaces (1 of them critical) because they were either turned off, not in use, or used only for training. Of the assessed 46 interfaces, 39 (85 percent) met information exchange requirements.

Of the 22 available critical interfaces that JITC assessed, 17 (77 percent) met information exchange requirements. Thus, 5 critical external interfaces (23 percent) did not meet the Net-Ready KPP threshold, which requires that every critical interface (100 percent) meet information exchange requirements. The systems that did not meet information exchange requirements are:

Standard Procurement System (two interfaces), Centralized Disbursing System (two interfaces), Departmental Management System, and Defense Department Reporting System.

- Centralized Disbursing System (CDS). CDS processes Air Force payments and collections and issues checks and electronic fund transfers. DEAMS has two defective interfaces with CDS:
  - CDS0-O-002. Severity 2. The Business Process Executable Language (BPEL) sometimes recycles the BPEL process and this takes over a day, invalidating transactions for the receiving system. No workaround exists.
  - CDS0-I-004. Severity 3. Errors in the BPEL cause the interface to run too long. This affects DEAMS ability to balance funds in a timely manner, but the interface still meets the basic need.
- Standard Procurement System (SPS). SPS provides standard business processes and data management (such as purchase orders and agreements) across disparate acquisition communities: DEAMS has two defective interfaces with SPS:
  - SPS0-I-001. Severity 2. Files with funded amounts are being captured as "Zero Dollar." This requires the Defense Finance and Accounting Service (DFAS) to load contract awards manually and reduces timeliness unless DFAS can note the situation and perform the manual workaround quickly.
  - SPS0-O-001. Under analysis. Outbound BPEL processes are faulting and causing problems in opening files.
- Departmental Cash Management System (DCMS). DCMS manages and reconciles cash disbursements, reimbursements, collections, and receipts and then sends the results to DEAMS. DEAMS has one defective interface with DCMS
  - DCMS-O-005. Severity 3. Bureau Control Numbers may be omitted when processing travel documents, which results in DEAMS receiving inaccurate or incomplete Accounts Payable and Accounts Receivable information.

JITC is working with the DEAMS FMO and Air Force Financial Systems Operations to validate the errors.

Training

DEAMS training, while improved somewhat since OA2, did not prepare users to employ DEAMS. The testers found that new users had very little knowledge of DEAMS. Some users only accessed DEAMS sporadically and did not develop or maintain proficiency. A long time gap between initial training and go-live also degraded user proficiency, as much of what was learned was forgotten. The training needs to align more closely with deployments rather than being given months in advance. This alignment could prove a challenge for presently scheduled deployments to many thousands of new users and scores of new bases over the next year.

Users indicated that the training focused on how to navigate within DEAMS rather than how to operate solely in the DEAMS environment and requested job-specific training that (1) is

up-to-date, (2) gives sufficient context as to what is being done and how to find related information, (3) relates to legacy processes appropriate for the student, and (4) provides hands-on experience with realistic scenarios in a timely manner. The business process changes that accompanied DEAMS implementation were inadequately explained, so users did not have a holistic understanding of how to accomplish their tasks. Additionally, more on-site technical support would have allowed them to better understand these processes and system requirements. In the OA2 report, DOT&E recommended that the Air Force modify DEAMS user training to focus more on functional understanding the DEAMS general ledger environment, rather than on navigation within the system. This has not been achieved.

To assist in training hundreds of new users, a few "power users" at each site received early DEAMS training prior to the general user training. Prior to that, most of them had completed optional computer-based training modules that gave them a measure of familiarity with DEAMS and helped them understand the classroom lessons that followed. Based on feedback from the power users, the completion of the computer-based training modules should be required before power user classroom training.

The power users struggled to maintain DEAMS proficiency after they returned to their bases. Although a DEAMS "sandbox" was available to practice on, the type of transactions available in the practice environment was not robust enough to maintain competency and the pressures of completing their missions in the day-to-day legacy system left little time for retention of DEAMS proficiency. Power users should be sent on short deployments to an existing DEAMS base soon after completion of classroom training so that their newly-learned skills can be reinforced by exposure to actual DEAMS use.

The largest group of users who reported that the training did not meet their needs were the "resource advisors" who are responsible for travel reimbursements. The resource advisors indicated that the training course did not prepare them to effectively execute their mission using DEAMS. The users noted that after months of lag between training and "go live", they were unable to execute reimbursements because DEAMS executes these functions fundamentally differently than the legacy system. Terminology differences between DEAMS and the legacy systems created a barrier to learning that could be mitigated with a glossary or similar product that relates DEAMS and legacy terminology and tailors training for this issue.

Just 53 percent of users rated the training as effective (119 out of 225 users surveyed), with a further 31 percent rating training as ineffective. Figure 4-6 displays user responses to the training effectiveness survey in which the median response was "slightly effective".

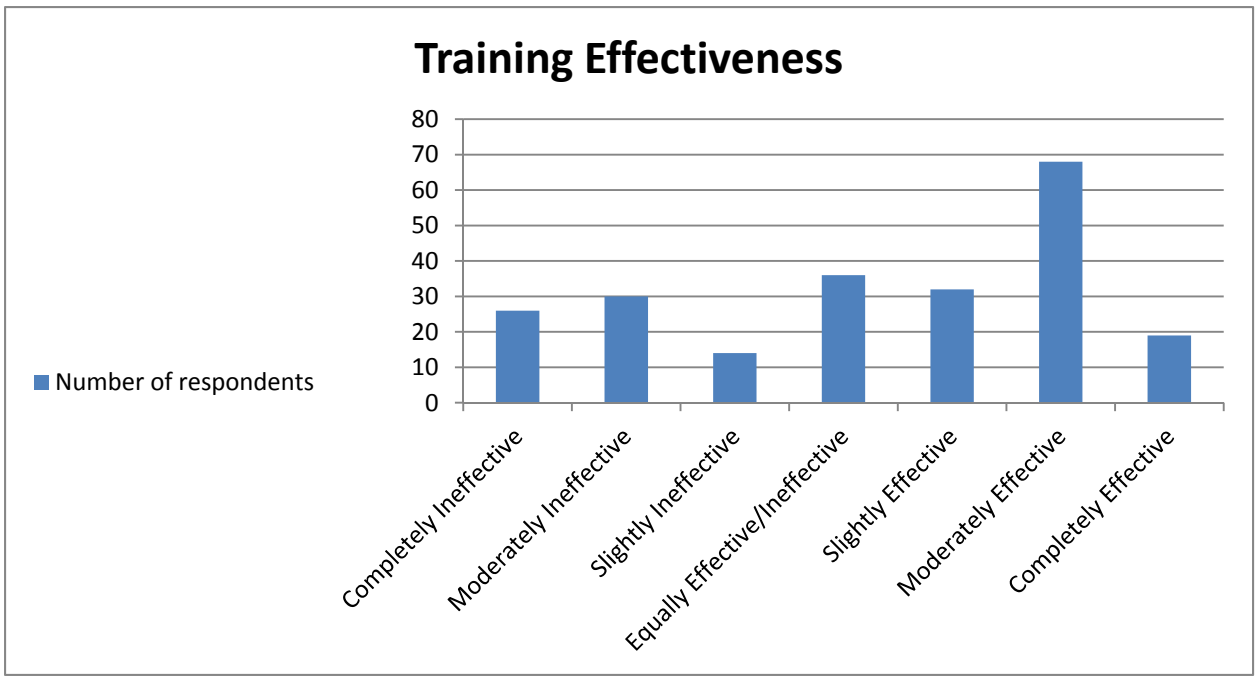


Figure 4-6. User Opinions of DEAMS Training

This page intentionally left blank.

Section Five
Cybersecurity

DEAMS is not survivable in the cybersecurity environment. Adversarial testing demonstrated that DEAMS did not protect information or detect cybersecurity threats. Operational evaluation of cybersecurity assesses the system's protect, detect, react, and restore capabilities and the mission effects induced by cyber threat activity. DEAMS did not protect critical information and did not detect adversarial intrusions. Because intrusions were not detected, there was no assessment of reaction to penetrations or restoration of the system after penetrations. DOT&E's assessment of cybersecurity is contained in the classified annex to this report.

This page intentionally left blank.

Section Six
Recommendations

The Air Force should implement the following recommendations to support the successful fielding of DEAMS Increment 1.

- Identify the root causes and processes, procedures and software improvements to clear the transaction backlog, which will fix the lag time between transaction and posting to ensure accurate reporting.
- Work with the Defense Finance and Accounting Service (DFAS) to identify root causes of imbalances between DEAMS and Treasury and change policies and procedures or recommend software improvements to prevent further imbalances.
- Conduct robust regression testing to improve DEAMS performance and identify potential interface issues prior to software updates and releases.
- Fix or effectively mitigate the deficiencies and cybersecurity vulnerabilities found during the IOT&E.
- Ensure that user training is designed to ensure users are prepared to use DEAMS at go-live and retain capabilities necessary to effectively use DEAMS.
- Conduct a Follow-on Operational Test and Evaluation before the Full Deployment Decision to verify correction of deficiencies found during the IOT&E and also to determine whether the Oracle Business Intelligence Enterprise Edition reporting tool is operationally effective, suitable, and cyber-secure prior to full deployment. Follow-on testing should include a repeat cyber vulnerability and penetration assessment to verify the fixes and mitigations for cybersecurity vulnerabilities.