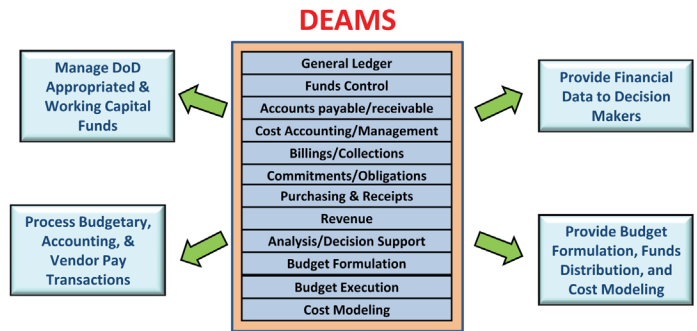# Defense Enterprise Accounting and Management System (DEAMS)

DEAMS

Executive Summary

- In accordance with a September 30, 2015, Acquisition Decision Memorandum, the Air Force Operational Test and Evaluation Center (AFOTEC) conducted a Verification of Fixes (VoF) test on the Defense Enterprise Accounting and Management System (DEAMS). AFOTEC planned to conduct the VoF test at four bases with the participation of three Air Force Major Commands, three U.S. Combatant Commands, and the Defense Finance and Accounting Service (DFAS), from January 4 – 29, 2016. However, the Program Executive Officer (PEO) stopped the VoF test after two bases (Scott AFB and Keesler AFB), when the data indicated that multiple Key Performance Parameters (KPPs) could not be met.
- The VoF test demonstrated that DEAMS remains not operationally effective and not operationally suitable. In the area of effectiveness, DEAMS Increment 1 did not effectively perform several critical accounting and management tasks, four of which were KPPs. DEAMS suitability issues included configuration management and usability as users continue to avoid using DEAMS to conduct financial analysis and reporting.
- DEAMS remains not survivable in the expected cybersecurity threat environment. Following IOT&E, the Program Management Office (PMO) conducted limited cybersecurity testing. From November 18 – 19, 2015, a cybersecurity test team conducted an event to assess three cybersecurity fixes. The team conducted this test on the live network in the pre-production environment, and verified that only one of the three fixes was successful. Subsequent cybersecurity testing demonstrated that another cybersecurity fix was successful on a single server in the DEAMS enclave. However, the cybersecurity deficiency still existed on two other servers in the enclave, indicating that the PMO's processes and procedures to prevent recurrence of cybersecurity problems are not yet adequate.

System

- DEAMS Increment 1 is a Major Automated Information System that uses commercial off-the-shelf Enterprise Resource Planning software to provide accounting and management services.
- The DEAMS Increment 1 PMO is following an evolutionary acquisition strategy that adds additional capabilities and users incrementally. There are six scheduled releases. The Air Force anticipates over 15,000 users worldwide will use DEAMS by the end of the increment.
- DEAMS Increment 1 is intended to improve financial accountability by providing a single, standard, automated financial management system that is compliant with the Chief Financial Officers Act of 1990 and other mandates. DEAMS Increment 1 performs the following core accounting functions:
  - Core Financial System Management
  - General Ledger Management
  - Funds Management
  - Payment Management
  - Receivable Management
  - Cost Management
  - Reporting
- DEAMS interfaces with approximately 40 other systems that provide travel, payroll, disbursing, transportation, logistics, acquisition, and accounting support.
- DEAMS supports financial management requirements in the Federal Financial Management Improvement Act of 1996 and DOD Business Enterprise Architecture. Therefore, DEAMS is a key tool for helping the DOD to have its financial statements validated as ready for audit by the end of FY17 as required by the National Defense Authorization Act for FY10.

Mission

Air Force financial managers and tenant organizations use DEAMS Increment 1 to do the following across the Air Force, U.S. Transportation Command, and other U.S. component commands:
- Compile and share accurate, up-to-the-minute financial management data and information
- Satisfy Congressional and DOD requirements for auditing of funds, standardizing of financial ledgers, timely reporting, and reduction of costly rework

Major Contractor

Accenture Federal Services – Dayton, Ohio

Activity

- In accordance with a September 30, 2015, Acquisition Decision Memorandum, AFOTEC conducted a VoF test on DEAMS. AFOTEC planned to conduct the VoF test at four bases with the participation of three Air Force Major Commands, three U.S. Combatant Commands, and DFAS, from January 4 – 29, 2016. However, the PEO stopped the VoF test after two bases (Scott AFB and Keesler AFB), when the data indicated that multiple KPPs could not be met. Therefore, AFOTEC completed testing at only two of the four test locations.
- In preparation for the VoF test, the Army Research Laboratory at White Sands Missile Range, New Mexico, supported the PMO in conducting a limited cybersecurity Cooperative Vulnerability and Penetration Assessment at Maxwell AFB – Gunter Annex, Alabama.
- The Joint Interoperability Test Command (JITC) completed a DEAMS Increment 1 interoperability evaluation in August 2016.
- AFOTEC conducted the VoF test in accordance with the DOT&E-approved Test and Evaluation Master Plan and the test plan.

Assessment

- DEAMS Increment 1 remains not operationally effective and not operationally suitable. DEAMS Increment 1 did not effectively perform several critical accounting and management tasks, four of which were KPPs. Some key effectiveness findings from the IOT&E and VoF test are as follows:
  - DEAMS does not provide an accurate balance of available funds to meet the KPP requirement. During the VoF test, only 62 percent (33 out of 53) of the balance queries were accurate, versus a 98 percent requirement.
  - DEAMS continues to have problems with interoperability with other systems, which contribute to the poor accuracy results discussed above. According to the August 2016 JITC interoperability report, four critical interfaces did not meet criteria due to timeliness problems which have a moderate to major impact on interoperability with two critical interfaces: the Centralized Disbursing System and Departmental Cash Management System.
  - Users continue to rely on the Commanders' Resource Integration System and other legacy systems for reporting instead of using the DEAMS Discoverer tool. Oracle Business Intelligence Enterprise Edition (OBIEE), the DEAMS replacement for Discoverer, has provided improved reporting capabilities on other programs (e.g., Defense Agencies Initiative), but challenges remain for implementation of OBIEE.
  - Transaction backlog continues to be a major problem with DEAMS. Transaction backlogs decreased during the summer of 2015, but increased in the fall and remained substantially above the low point seen during the previous months. At the start of the VoF test, the transaction backlog was near 20,000 transactions.

  - In both the IOT&E and VoF, the transaction backlog was a major contributor to the inadequate performance of DEAMS. The transaction backlog causes a transaction to take longer than normal to post on the General Ledger, which in turn causes inaccuracies in DEAMS reports, to include the Status of Funds.
  - Depending upon the type of backlogged transaction, an un-posted transaction can result in interest penalty payments on aged transactions, affecting timely decision-making and requiring additional manpower for DFAS staff to process backlog transactions.
- Numerous high-severity incident reports, deficiencies, and system change requests (SCRs) remain. The numbers of Severity 2 and 3 defects and SCRs are noted in Table 1 (Severity 2 problems adversely affect DEAMS and do not have a sustainable work around, while Severity 3 problems adversely affect DEAMS but have a sustainable work around). Of the 114 unresolved defects reported by the DEAMS Functional Management Office as of July 2016, 55 (48 percent) were over 8 months old. Of the 318 SCRs reported as of July 2016, 217 (68 percent) were over 8 months old.

Table 1: Defects and SCRs from prior to and after VoF		
	November 2015	July 2016
Severity 2 Defects	52	34
Severity 3 Defects	174	68
Severity 2 System Change Requests (SCRs)	52	96
Severity 3 SCRs	204	186

- The DEAMS PMO is not following its own configuration management procedures, which prescribe rigorous developmental and regression testing prior to fielding new software releases. The PMO sharply reduced developmental and regression testing starting in August 2014 to meet a fixed deployment schedule. This led to the fielding of defective software; this software is likely a major contributor to the backlog problems that continue to affect DEAMS users. DEAMS regression testing has recently increased to cover close to 60 percent of the business processes. The PMO should implement regression scripts to test all critical interfaces in DEAMS.
- Where it is possible to do so, users continue to avoid using DEAMS to conduct financial analysis and reporting. For example, Keesler AFB users export DEAMS data to spreadsheets to perform analyses and reporting rather than use corresponding DEAMS functionality. Additionally, PMO data from the months of September and October 2015 indicate that users generated Status of Funds reports less than once per week on average per user. These reports are critical to end-of-month and fiscal year-end closeouts; therefore, these data indicate that most of the approximately 11,000 DEAMS

users are using legacy systems instead of DEAMS to evaluate fund status.

- DEAMS remains not survivable in the expected cybersecurity threat environment. Following IOT&E, the PMO conducted limited cybersecurity testing. From November 18 – 19, 2015, a cybersecurity test team conducted a limited event to assess three cybersecurity fixes. The team conducted this test on the live network in the pre-production environment, and verified that only one of the three fixes was successful. Subsequent cybersecurity testing demonstrated that another cybersecurity fix was successful on a single server in the DEAMS enclave. However, the cybersecurity deficiency still existed on two other servers in the enclave. This indicates that the PMO's processes and procedures to prevent recurrence of cybersecurity problems are not yet adequate. However, the PMO instituted improved cybersecurity processes by adding the cybersecurity problems to the deficiency management system for visibility and action, instituted dedicated cybersecurity patch releases, and reprioritized all cybersecurity findings for correction or risk acceptance.

Recommendations

- Status of Previous Recommendations. The Program Office did not satisfy the FY15 recommendations to:
  1. Correct balance accuracy defects in accordance with KPP requirements and demonstrate progress towards DEAMS Increment 1 achieving full auditability.
  2. Identify and implement processes, procedures, and software improvements to clear the transaction backlog to fix the lag time between transaction and posting of transaction, and to ensure accurate and timely reporting.

3. Conduct regression testing to improve DEAMS Increment 1 performance and identify potential interface problems before fielding software updates and releases.
4. Provide DEAMS Increment 1 training that prepares users to effectively employ DEAMS Increment 1 upon fielding.
5. Work with AFOTEC to conduct follow-on operational testing to verify that the deficiencies have been corrected and that the new reporting tool is operationally effective, suitable, and survivable, once corrections have been made and a new reporting tool has been fielded.

- FY16 Recommendations. The DEAMS Program Manager should:
  1. Cease allowing DEAMS to be schedule-driven and delay DEAMS deployments, until the PMO fixes the backlog of high-severity deficiencies and shows that the system works properly during operationally realistic testing.
  2. Determine the root causes of the transaction backlogs and other anomalies that have appeared since the fielding of deficient software in August 2014 and make a concerted effort to clear remaining backlogs.
  3. Conduct FOT&E with a pilot set of users, prior to further deployments, to confirm DEAMS is operationally effective, operationally suitable, and survivable.
  4. Complete integration and testing of the OBIEE reporting tool and demonstrate effectiveness through operational testing to allow the retirement of Discoverer and fielding of OBIEE.
  5. Develop necessary regression testing scripts to ensure that all critical DEAMS interfaces are adequately tested.
  6. Complete mitigation of all cybersecurity vulnerabilities.