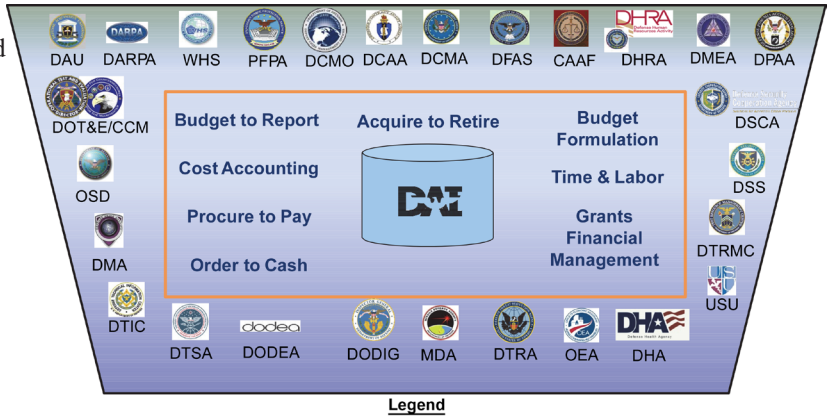
Defense Agencies Initiative (DAI)

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted IOT&E of Defense Agencies Initiative (DAI) Increment 2 from March 6 through April 7, 2017.
  - During the IOT&E, JITC evaluated new and existing capabilities implemented by DAI-equipped defense agencies, DOD field activities, and other defense organizations (collectively referred to here as Agencies).
  - JITC also evaluated new functionality for Agencies that recently migrated to DAI (Defense Security Cooperation Agency, DOD Inspector General, Defense Human Resources Activity, and DOT&E).
- DAI is operationally effective and operationally suitable, and has made improvements compared to previous test and evaluation events.
  - During this IOT&E and the previous operational assessments (OAs), DAI successfully completed 99 percent of the users' critical tasks in seven business process areas.
  - During this IOT&E, DAI demonstrated improved operational reliability and availability as compared to the previous OAs; however, the system continues to require improvements in usability.
  - Help desk metrics indicate the DAI system is sustainable. However, most Agencies provide additional funding to sustain Tier 1 (local) help desk support, training, and support for new capability development, which masks the true cost of DAI sustainment for the DOD enterprise.
- JITC and the Defense Information Systems Agency (DISA) Risk Management Executive Red Team conducted a Cooperative Vulnerability and Penetration Assessment (CVPA), an Adversarial Assessment, and a Cyber Economic Vulnerability Assessment (CEVA) from March 6 to May 19, 2017, to test the cybersecurity of DAI.
  - DAI is secure from an outsider cyber threat having limited capabilities; however, DAI is vulnerable to an insider cyber threat operating with limited to moderate capabilities.
  - Program defenders failed to detect and react to Red Team activities.
- DAI's continuity of operations (COOP) tabletop exercise in 2017 verified that the alternate site could restore partial mission or business processes. The ability of the alternate site to provide required performance levels under load and then restore full capability to the primary site remains unknown until DAI conducts a full COOP event.



Legend

CAAF - Court of Appeals for the Armed Forces
DAI - Defense Agencies Initiative
DARPA - Defense Advanced Research Projects Agency
DAU - Defense Acquisition University
DCAA - Defense Contract Audit Agency
DCMA - Defense Contract Management Agency
DCMO - Deputy Chief Management Officer
DFAS - Defense Finance and Accounting Service
DHA - Defense Health Agency
DHRA - Defense Human Resources Activity
DMA - Defense Media Activity
DMEA - Defense Microelectronics Activity
DODEA - Department of Defense Education Activity
DODIG - Department of Defense Inspector General
DOT&E/CCM - Director, Operational Test & Evaluation including Center for Countermeasures (CCM)
DPAA - Defense Prisoner of War/Missing In Action Accounting Agency
DSCA - Defense Security Cooperation Agency
DSS - Defense Security Service
DTIC - Defense Technical Information Center
DTRA - Defense Threat Reduction Agency
DTRMC - Defense Test Resource Management Center
DTSA - Defense Technology Security Administration
MDA - Missile Defense Agency
OEA - Office of Economic Adjustment
OSD - Office of the Secretary of Defense
PFPA - Pentagon Force Protection Agency
USU - Uniformed Services University of the Health Sciences
WHS - Washington Headquarters Services

System

- DAI is an integrated financial management solution that provides a real-time, web-based system of integrated business processes used by defense financial managers, program managers, auditors, and the Defense Finance and Accounting Service. The DAI core functionality is based on the Oracle E-Business Suite (currently release 12.2.5), which is a commercially available enterprise solutions system.
- DAI subsumes many systems and standardizes business processes for multiple DOD Agencies. It modernizes these processes by streamlining management capabilities to address financial reporting material weaknesses, and support financial statement auditability.
- DISA provides facilities, network infrastructure, and the hardware operating system for DAI servers at its Ogden, Utah, and Columbus, Ohio, Defense Enterprise Computing Centers.
- Agencies employ DAI worldwide and across a variety of operational environments via a web portal on the Non-classified Internet Protocol Router Network using each Agency's existing information system infrastructure.
- DAI includes two software increments with a third in planning for future fielding:
  - Increment 2 replaced Increment 1 and has four software releases, each adding capabilities and deploying to additional Agencies. With the completion of Increment 2 Release 4 fielding in October 2017, DAI provides services to 22 Agencies with 39,342 users at 1,148 locations worldwide.
  - The DAI Program Management Office (PMO) is planning for Increment 3 to provide additional capabilities

to existing Agencies and to add DISA, the Defense Commissary Agency, and potentially other Agencies from FY19 through FY23.
- DAI supports financial management requirements in the Federal Financial Management Improvement Act and DOD Business Enterprise Architecture and is a key tool for helping DOD Agencies have their financial statements validated as ready for audit.

Mission

Financial Managers in defense agencies use DAI to transform their budget, finance, and accounting operations to achieve accurate and reliable financial information in support of financial accountability and effective and efficient decision-making.

Major Contractors
- CACI Arlington – Arlington, Virginia
- International Business Machines – Armonk, New York
- Northrop Grumman – Falls Church, Virginia

Activity
- The DAI PMO conducted six developmental test events in FY17:
  - DAI Increment 2 Release 3.1
    - Development integration test from December 16, 2016, through March 3, 2017
    - System integration test from March 13 through April 7, 2017
    - User acceptance test from May 8 through June 2, 2017
  - DAI Increment 2 Release 4
    - Development integration test from March 29 through June 21, 2017
    - System integration test from June 22 through July 28, 2017
    - User acceptance test from August 3 through September 8, 2017
- In coordination with DISA, the DAI PMO conducted its annual COOP tabletop exercise on January 26, 2017. Neither JITC nor DOT&E were invited by the DAI PMO to observe the event, so DAI's COOP capability remains unassessed by DOT&E.
- From March 6 through April 7, 2017, JITC conducted an IOT&E of DAI Increment 2, in accordance with a DOT&E-approved test plan.
- From March 6 through May 19, 2017, JITC and the DISA Risk Management Executive Red Team completed a CVPA, an Adversarial Assessment, and a CEVA to test the cybersecurity of DAI. The DAI PMO deferred the data fraud analysis portion of the CEVA until Increment 3 testing.
- On June 29, 2017, the USD(AT&L) signed an Acquisition Decision Memorandum establishing DAI Increment 3 and authorizing the PMO to conduct analysis activities in preparation for an Authority to Proceed decision review.
- DOT&E published its "Defense Agencies Initiative Increment 2" IOT&E report in September 2017.
- Based on DOT&E recommendations and emerging results of the IOT&E, the DAI PMO created a dedicated "Customer Liaison" relationship with each Agency. The goal of the relationship is to provide greater focus on particular problem areas within each Agency, with the overall objective of reducing Tier 2 help desk tickets (i.e., Tier 2 tickets are incidents that require support from technicians with great technical knowledge of DAI and the Tier 2 help desk is staffed by technicians who have troubleshooting capabilities beyond the Tier 1 support at the Agencies).
- JITC and the DAI PMO are planning an FOT&E and a cybersecurity test during 2Q-3QFY18. The FOT&E will focus on new Agencies (high-priority Measures of Performance only), new functionality, and those Measures of Performance that were not tested or that were inconclusive at the end of IOT&E. The cybersecurity testing will consist of a validation of corrected findings from IOT&E, Adversarial Assessment, and COOP.
- On October 3, 2017, the USD(AT&L) signed the DAI Increment 2 and 3 Acquisition Decision Memorandum (ADM). The memorandum authorized the full deployment of DAI Increment 2 and development activities for DAI Increment 3.

Assessment
- DAI is operationally effective and has made significant improvements compared to previous test and evaluation events.
  - During the Increment 2 IOT&E and previous two OAs combined, DAI successfully completed 2,054 of 2,073 critical tasks (99 percent). The 19 unsuccessful tasks include hardware, software, or system errors that the PMO has corrected, and user errors that better training and user documentation could address.
  - Two system failures occurred over a 6-month period from November 2016 to April 2017 and the mean time between system failures was 2,004 hours. The mean time to repair the two system failures was 2.05 hours, and operational availability was 93 percent. Ten scheduled maintenance periods, averaging 30.2 hours, affected operational availability. Inherent system availability, which does not include scheduled downtime, was 99 percent, meeting system requirements.
  - The DAI PMO has a goal of one 27-hour maintenance period completed during one weekend per month.

Achieving that goal would improve operational availability to 96 percent. This would better support worldwide operations and improve weekend operations during peak periods, especially during the critical closeout period near the end of the fiscal year.

- DAI is operationally suitable; however, the program has not made gains in operational suitability that would correspond with those realized in operational effectiveness.
  - The DAI Increment 2 Business Case defines the High Level Outcomes (HLOs), which quantitatively establish the value added by DAI Increment 2. During the IOT&E, the HLO dashboard in DAI reported on 6 of 18 HLOs. In some cases, Agencies are not using the full suite of Increment 2 capabilities, are not monitoring the HLO dashboard, and have not achieved the HLO thresholds. DOT&E will reassess the HLOs during Increment 3 testing.
  - In spite of the improvements in the DAI system, users continue to give the program a marginal System Usability Score of 54, up from 48 reported in the Release 2 OA. Factors causing that marginal user rating include:
    - Experience is a statistically significant factor. Four out of 16 Agencies surveyed during IOT&E had used DAI for less than 2 years. Users at those four Agencies assessed usability to be unacceptable (less than 50). Users with more experience scored DAI higher.
    - Frequent user comments on DAI functionality related to the slowness and difficulty of entering data and generating DAI reports, queries, and search requests.
  - DAI Help Desk support for the Agency help desks is sustainable, but most Agencies provide additional funding to obtain additional manning for help desk support, training, and support for new capability development. This user funding masks the true cost of DAI sustainment for the DOD enterprise.
  - The DAI Help Desk processed 6,479 service requests or incidents between November 1, 2016, and April 1, 2017, with the number of open tickets decreasing from 690 to 523 over that period.
  - The DAI PMO resolved 81 percent (525 of 647) Priority 2 tickets within 30 days. Customer satisfaction with the DAI Help Desk was 68 percent, compared to 92 percent for the local Agency help desk support. The DAI Tier 2 Help Desk provides users with workarounds to all Priority 2 issues until a permanent resolution is determined. Improving resolution times for Priority 2 issues should improve overall customer satisfaction.
- DAI is secure against an outsider cyber threat having limited capabilities; however, DAI is vulnerable to an insider cyber threat operating with limited to moderate capabilities.
  - During the Adversarial Assessment, the DISA Red Team – using limited cyber-attack capabilities – was unable to exploit DAI as an outsider. However, as an insider, the Red Team identified four vulnerabilities, and the network defenders did not detect the Red Team.
- During the CEVA, Agencies' financial experts concluded that the existing technical checks would make it difficult to exploit known or potential vulnerabilities to commit fraud.
- Per DISA and Defense Logistics Agency Chief Information Officer policy, the DAI PMO conducts a remote recovery exercise once every 3 years, with a tabletop exercise conducted in the years between.
- During the FY17 COOP exercise, the DAI PMO and DISA conducted a tabletop exercise where personnel reviewed and updated the Information Security Contingency Plan. Previously in FY16, DAI PMO testers successfully executed selected business functions on alternate site servers, which verified that the alternate site could restore partial mission or business essential functionality. Because of the limited number of users and tasks, testing did not include load or performance testing. The alternate site does not currently have the capacity to support a full service restoration of DAI capabilities.

Recommendations

- Status of Previous Recommendations. The program has implemented changes to address many of the FY16 recommendations; however, the following recommendations remain applicable:
  1. DISA and DAI personnel failed to detect and react to Red Team activities during two consecutive Adversarial Assessments; therefore, DAI should work with DISA to improve real-time cybersecurity detect and react capabilities for DAI and mitigate known vulnerabilities.
  2. The PMO still needs to conduct the fraud analysis portion of the CEVA. It is currently planned for the first operational assessment of DAI Increment 3 in FY19.
  3. The DAI PMO should continue to monitor and improve system performance to reduce response times and unexpected errors.
- FY17 Recommendations. The full list of recommendations is available in the September 2017 DOT&E report on DAI IOT&E; highlighted recommendations are below. The DAI PMO should:
  1. Complete the HLO dashboard by working with the Office of the Under Secretary of Defense (Comptroller) to identify who manages the Agencies as they reengineer business processes to achieve HLO standards.
  2. Maintain "Customer Liaison" positions within the PMO to consolidate and share lessons learned with the Agencies as they implement DAI.
  3. Improve real-time cybersecurity detect and react capabilities for DAI and verify fixes during the FY18 FOT&E.
  4. Decrease the time to resolve DAI PMO Help Desk tickets.
  5. Continue to improve COOP site architecture and capabilities with a goal of developing a full DAI restoration capability from COOP to production site.
  6. Coordinate for all DAI Agencies participation in the next annual COOP event, with JITC and DOT&E observing.