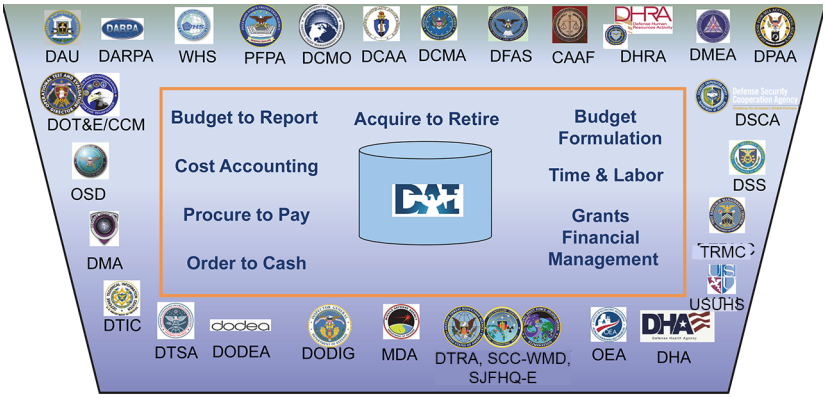
Defense Agencies Initiative (DAI)



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
DTSA - Defense Technology Security Administration
JSTO - Joint Science and Technology Office
MDA - Missile Defense Agency
OEA - Office of Economic Adjustment
OSD - Office of the Secretary of Defense
PFPA - Pentagon Force Protection Agency
SCC-WMD - US Strategic Command Center for Combatting Weapons of Mass Destruction
SJFHQ-E - Standing Joint Force Headquarters-Elimination
TRMC - Test Resource Management Center
USU - Uniformed Services University of the Health Sciences
WHS - Washington Headquraters Services

Executive Summary

- The Joint Interoperability Test Command (JITC) conducted an operational assessment (OA) of the Defense Agencies Initiative (DAI) Increment 2 Release 2 from February 29 through March 18, 2016. During this OA, DAI successfully completed 98 percent of the users' critical tasks.
- During the OA, the DAI Program Management Office (PMO) provided data for only one of six high-level outcomes (HLOs) with defined measures.
- Both DAI's operational reliability and availability during the OA improved as compared to the previous OA; however, the system continues to require improvements in usability.
- During its cybersecurity testing, DAI was difficult to exploit by an outsider threat but was vulnerable to an insider threat with administrator credentials. Neither DAI nor the network defenders detected Red Team activity or an event designed to artificially stimulate a reaction.
- DAI's annual continuity of operations (COOP) exercise verified that the alternate site could restore partial mission or business processes, but hosting limitations prohibits the system from efficiently reconstituting back to the primary DAI site.

System

- DAI is an integrated financial management solution that provides a real-time, web-based system of integrated business processes and is used by defense agency financial managers, program managers, auditors, and the Defense Finance and Accounting Service (DFAS). DAI's core functionality is based on Oracle E-Business Suite Release 12.2.3 (a commercially available enterprise solutions system).
- DAI subsumes many systems and standardizes business processes for multiple DOD agencies and field activities. It modernizes the financial management processes by streamlining financial management capabilities, addressing financial reporting material weaknesses, and supporting financial statement auditability.
- The Defense Information Systems Agency (DISA) provides facilities, network infrastructure, and the hardware operating system for the DAI servers at its Ogden, Utah, and Columbus, Ohio, Defense Enterprise Computing Centers.
- DAI is employed worldwide and across a variety of operational environments via a web portal on the Non-secure Internet Protocol Routing Network (NIPRNET) using each agency's existing information system infrastructure.

- DAI includes two software increments:
  - Increment 2 replaces Increment 1 and is in use for financial reporting at 12 defense agencies.
  - Increment 2 has four software releases, each with additional capabilities, with deployments to 15 additional defense agencies continuing through FY17. With the completion of Release 2.2 fielding on June 20, 2016, DAI provides services to 20 defense agencies and field activities with 29,852 users at 856 locations worldwide.
- DAI supports financial management requirements in the Federal Financial Management Improvement Act and DOD Business Enterprise Architecture. Therefore, it 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

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 decision making.

Major Contractors

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

Activity

- From November 16, 2015, to May 31, 2016, JITC and the DISA Risk Management Executive Red Team completed a Cooperative Vulnerability and Penetration Assessment, an Adversarial Assessment, and a Cyber Economic Vulnerability Assessment (CEVA) to test the cybersecurity of DAI.
- From February 29 through March 18, 2016, JITC conducted an OA of DAI Increment 2 Release 2, in accordance with a DOT&E-approved test plan. The test was adequate, except the CEVA data fraud analysis portion, which JITC deferred until the IOT&E.
- The DAI PMO conducted three developmental test events of DAI Increment 2 Release 3 throughout FY16: a development integration test from January 6 through July 28, 2016; a system integration test from June 20 through July 28, 2016; and a user acceptance test conducted from August 2 through September 8, 2016.
- In coordination with DISA, the DAI PMO conducted its annual COOP exercise from April 25 – 29, 2016. As the hosting agency for DAI, DISA provides a mix of tabletop and remote recovery and simulation exercises to meet the program's system requirements.
- On October 7, 2016, USD(AT&L) signed an Acquisition Decision Memorandum approving limited fielding of DAI Increment 2 Release 3 to current and additional defense agencies.
- On November 9, 2016, USD(AT&L) signed an Acquisition Decision Memorandum approving development of DAI Increment 2 Release 4 with current and additional defense agencies.
- JITC and the DAI PMO are coordinating for a full cybersecurity test (Cooperative Vulnerability and Penetration Assessment, Adversarial Assessment, CEVA, and COOP) for 2Q – 3QFY17 as part of the IOT&E on Increment 2 Release 3.

Assessment

- During the Release 2 OA, DAI successfully completed 669 of 682 critical tasks (98 percent). The 13 unsuccessful tasks include hardware, software, or system errors that have been corrected and user errors that better training and user documentation could address.
- Comparing DAI's performance during the Release 2 OA to the Release 1 OA, the mean time between system failure improved from 292 to 328 hours and operational availability improved from 83 to 89 percent. The DAI PMO more closely managed scheduled maintenance to increase reliability and availability to users worldwide.
- Users opened 13 critical-level problem tickets from November 1, 2015, to March 18, 2016, and the DAI PMO resolved all within 4 days. Users also opened 189 major-level problem tickets during the same timeframe; by May 10, 2016, the DAI PMO had resolved all but 5 of the tickets.
- The DAI Increment 2 Business Case defines the HLOs, which quantitatively establish the value added by DAI Increment 2. However, of the six HLOs with defined measures, JITC measured only "Automate Absence Management" during the Release 2 OA. During the IOT&E, the DAI PMO must provide data for the remaining HLOs in order to provide a detailed, realistic assessment of the effectiveness of the program.
- In spite of the improvements in the DAI system, users gave the program a System Usability Score of 48, down from 59 reported in the Release 1 OA. Factors causing that decline include:
  - There was a 15 percent increase in DAI users with less than 2 years of experience with the system. Those users scored DAI lower than users with more experience.
  - Frequent user comments on DAI functionality related to the slowness and difficulty to enter data and generate DAI reports, queries, and search requests.
- During the Adversarial Assessment, the DISA Red Team – using limited to moderate cyber-attack capabilities – was unable to exploit DAI as an outsider or as an insider with user-level credentials. However, as an insider with administrator-level access, the Red Team identified four vulnerabilities. Neither DAI nor the network defenders

detected the Red Team or an event designed to artificially stimulate a reaction.
- 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.
- During the COOP exercise, 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 users and tasks, testing did not include load or performance testing. At present, DISA does not provide reconstitution (failover) as a service which precludes DAI from performing a full reconstitution exercise for the COOP environment.

Recommendations
- Status of Previous Recommendations. The program has implemented changes to address the FY15 recommendations, but the fraud analysis portion of the CEVA was deferred until the IOT&E.
- FY16 Recommendations. The DAI PMO should:
  1. Improve system performance to reduce response times and unexpected errors.
  2. Provide high-level outcome data to JITC both before and during the IOT&E for evaluation of operational effectiveness.
  3. Improve training and documentation to include error message handling, reports and queries in DAI or Oracle business intelligence, and other advanced training courses.
  4. Work with DISA to improve real-time cybersecurity detect and react capabilities for DAI and mitigate known vulnerabilities.
  5. Improve COOP site architecture and capabilities with a goal of developing a data replication capability from COOP to production site.