Executive Summary

- The Joint Interoperability Test Command (JITC) conducted FOT&E of Defense Agencies Initiative (DAI) Increment 2 from March 5 through April 6, 2018.
  - During the FOT&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 (Washington Headquarters Services and Defense Contract Audit Agency).
- DAI is operationally effective. The system successfully completed 99 percent of all critical tasks within 7 business process areas throughout all operational testing.
- Operational suitability for DAI is marginal. Overall system availability was high and DAI supported the audit readiness of the DOD; however, usability and system responsiveness ranged from marginal to not acceptable.
  - Limited regression testing of a security patch to address an Information Assurance Vulnerability Alert (IAVA) led to increased sporadic system latency during FOT&E.
- Based on the System Usability Scale Survey for 7 out of 22 Agencies using DAI, Agencies that migrated to DAI during Increment 1 assessed DAI usability as marginal and Agencies that migrated to DAI during Increment 2 assessed DAI usability as not acceptable.
- DAI exceeded system availability requirements with 99 percent system availability.
- Agency representatives responsible for audit readiness agree that DAI supports audit readiness through its financial reporting and transaction traceability.
  - Help desk metrics indicate the DAI system is sustainable. However, most Agencies provide additional funding to sustain Tier 1 (local) help desk support, functional and system training, and support for new capability development, which masks the true cost of DAI sustainment for the DOD enterprise.
- JITC and the Defense Logistics Agency Information Operations, Cybersecurity (J61) Penetration Test Team conducted a modified Cooperative Vulnerability and Penetration Assessment (CVPA) from February 12 to March 16, 2018, to verify remediation of open findings from previous cybersecurity testing.
  - Based on previous testing and the remediation of five of six open findings, DAI is secure against a cyber threat having limited to moderate capabilities. However, the overall survivability assessment remains undetermined until the final open finding is remediated and verified.

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 commercially available enterprise resource planning solutions.
- DAI subsumes many systems and standardizes business processes for multiple DOD Agencies. It modernizes these business processes by streamlining management capabilities to address financial reporting material weaknesses, and support financial statement auditability.
- The Defense Information Systems Agency (DISA) provides facilities, network infrastructure, and the hardware operating system for DAI servers at DISA data centers.
- Agencies employ DAI worldwide and across a variety of operational environments via a web portal using each Agency’s existing information system infrastructure.
- The DAI program is delivering capability incrementally:
  - Increment 2 had 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) has begun development and fielding of Increment 3 to provide additional capabilities to existing Agencies and to add DISA, the Defense Commissary Agency, and potentially other Agencies from FY18 through FY23. DISA went live with Time and Labor capabilities in June 2018 as part of Increment 3 Release 0.1, and increased the DAI user base to 45,725 users at 1,834 locations worldwide.

- 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, Virginia
- International Business Machines – Armonk, New York
- Northrop Grumman – Falls Church, Virginia
- Intellipoint Consulting, Inc. – Ashburn, Virginia

**Activity**

- On October 3, 2017, the USD(AT&L) issued a Full Deployment Decision for DAI Increment 2 and a development Authority to Proceed for DAI Increment 3.
- The DAI PMO conducted six developmental test events in FY18:
  
  **DAI Increment 3 Release 0.1**
  
  - Development integration test from December 22, 2017, through March 2, 2018
  - System integration test from March 12 through April 6, 2018
  - User acceptance test from May 7 through June 1, 2018

  **DAI Increment 3 Release 1**
  
  - Development integration test from March 30 through June 12, 2018
  - System integration test from June 25 through July 27, 2018
  - User acceptance test from August 6 through September 7, 2018

  - In coordination with DISA, the DAI PMO conducted its annual Continuity of Operations (COOP) tabletop exercise on January 19, 2018. Both JITC and DOT&E observed the event and assessed the DAI COOP capability as meeting requirements. DAI PMO briefed the COOP results to all Agencies with no concerns noted.
  - From March 5 through April 6, 2018, JITC conducted an FOT&E of DAI Increment 2 in accordance with a DOT&E-approved test plan. Interoperability Certification data were collected from November 2017 through May 2018.
  - From February 13 through March 16, 2018, JITC and the Defense Logistics Agency (DLA) Information Operations, Cybersecurity (J61) Penetration Test Team conducted a modified CVPA to verify that actions taken by the DAI PMO successfully corrected open findings from IOT&E. The DAI PMO deferred the data fraud analysis portion of the Cyber Economic Vulnerability Assessment (CEVA) until Increment 3 testing.
  - JITC and the DAI PMO are planning an operational assessment (OA) and cybersecurity testing during 2Q-3QFY19 for Increment 3 Release 1. The OA will focus on new Agencies, new functionality, and those measures of performance that were not tested or that were inconclusive at the end of Increment 2 testing. The cybersecurity testing will consist of a validation of corrected actions based upon findings from Increment 2 testing, a CVPA, an Adversarial Assessment, and a COOP exercise.
  - On September 26, 2018, the USD(A&S) issued an Acquisition Decision Memorandum delegating Milestone Decision Authority to DLA for DAI Increment 3 and all future program increments.

**Assessment**

- DAI is operationally effective and has made significant improvements compared to previous T&E events.
  - During the Increment 2 FOT&E, IOT&E, and two OAs combined, DAI successfully completed 2,447 of 2,466 critical tasks (99 percent). The 19 unsuccessful tasks included hardware, software, or system errors that the PMO has corrected, and user errors that better training and user documentation could address.
  - The DAI Increment 2 Business Case defines the High Level Outcomes (HLOs) that establish the rationale for DAI Increment 2. During the FOT&E, DAI reported on 11 of 18 HLOs. In some cases, Agencies are not using the full suite of Increment 2 capabilities, are not monitoring the HLO dashboard, or have not achieved the HLO thresholds. DOT&E will reassess the HLOs during Increment 3 testing.
  - DAI Increment 2 added functionality for Budget Formulation and Grants Financial Management Accounting, but the PMO has yet to measure the effectiveness of those functionalities. DAI Budgeting Formulation is still maturing with five Agencies levering the capability.
  - The operational suitability for DAI is marginal. Auditability, reliability, availability, maintainability, and sustainability of the help desk support were all acceptable. However, the
mission effects from periods of high system latency resulted in
not acceptable user experiences.
- The DAI PMO introduced a software security patch in
  January 2018 that resulted in sporadic system latency.
Correcting the system required several planned and
unplanned maintenance outages during the test period,
negatively affecting users. Automated regression testing
and performance testing could reduce the risk of future
patches negatively affecting the production environment.
- DAI exceeded system availability requirements with
  99 percent system inherent availability. System inherent
availability is the percentage of time a system is available,
while operational availability is the percentage of time
that a system is capable of performing its mission. DAI
also exceeded the performance requirements for other
reliability, availability, and maintainability measures during
FOT&E. Ten system failures occurred over a 6-month
period from November 2017 to April 2018 and the mean
time between system failures was 410 hours. The mean
time to repair the 10 system failures was 4.5 hours. The
11 scheduled maintenance periods and the 10 unplanned
maintenance periods averaged 14 hours each and resulted
in an operational availability of 93 percent.
- 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.
- In spite of the improvements in the DAI system, users
  continue to give the program a marginal System Usability
Scale score. Users from the three Increment 1 Agencies
surveyed assessed usability as marginal, whereas users
from the four Increment 2 Agencies surveyed assessed
usability as not acceptable. Factors causing the not
acceptable user ratings include:
  • Experience is a statistically significant factor. Four out
    of seven Agencies surveyed during FOT&E had used
DAI for less than 3 years. Users at those four Agencies
assessed usability to be not acceptable (less than
50 percent). Agencies with more experience scored DAI
higher.
  • Frequent user comments on DAI functionality related
to system slowness and difficulty of entering data and
generating DAI reports, queries, and search requests.
  • Sporadic system latency during January and
    February 2018 from an operating system security patch to
address an IAVA resulted in poor user experiences.
- DAI Help Desk support for the Agency help desks is
acceptable, but most Agencies provide additional funding
to obtain additional staff 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 6,850 service requests
between November 1, 2017, and May 1, 2018, with the
number of open tickets increasing from 697 to 821 during
that period. Although the DAI Help Desk is sustainable,
the DAI PMO needs to allocate more resources so that the
ticket resolution rate (37 per day) is on par with the ticket
submission rate (38 per day).
- Customer satisfaction with the DAI Help Desk was
  77 percent, compared to 75 percent for the local Agency
help desk support.
  • DAI is secure against a cyber threat having limited to moderate
  capabilities, but the overall survivability assessment remains
undetermined since more testing is required.
- During the modified CVPA, JITC and the DLA Information
  Operations, Cybersecurity (J61) Penetration Test Team
verified that the DAI PMO had corrected five out of the six
findings from the IOT&E Adversarial Assessment.
- JITC did not test the cybersecurity defender’s ability to
detect and mitigate Red Team activities; therefore, net
defense will remain unassessed until the Adversarial
Assessment during Increment 3 testing.
- During the Increment 2 CEVA, Agencies’ financial experts
concluded that the existing technical checks would make it
difficult to exploit known or potential vulnerabilities to commit
fraud. DOT&E is monitoring the DOD Inspector General
FY18-19 Financial Audits of Agencies on DAI to assist with
CEVA requirements.
- Per DISA and DLA 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 both the FY17 and FY18 COOP exercises, 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 mission
essential business functionality. DAI will test select business
functions at the alternate site in January 2019.

Recommendations
The full list of recommendations is available in the
November 2018 DOT&E DAI FOT&E report.
The DAI PMO should:
1. Improve both regression and performance testing in order to
   reduce the risk of introducing misconfigured code into the
   production environment.
2. Work with the Office of the Under Secretary of Defense
   (OUSD) Comptroller to mature DAI budget formulation
capabilities.
3. Work with DISA to improve system responsiveness.
4. Along with OUSD Comptroller and the Agencies, track the
   progress of the Agencies and the Department to achieve
   HLO thresholds.
5. Allocate more resources so that the ticket resolution rate is
   at least on par with the ticket submission rate.
6. In conjunction with JITC, measure system responsiveness during operational testing to quantify the latency problems identified through user survey responses during Increment 2 testing.