

Primary Recommendation B2
Automated Testing and Evaluation

<i>Line of Effort</i>	Create and maintain cross-program/cross-service digital infrastructure.		
<i>Recommendation</i>	Create, implement, support, and use fully automatable approaches to testing and evaluation (T&E), including security, that allow high-confidence distribution of software to the field on an iterative basis.		
<i>Stakeholders</i>	DOT&E, USD(A&S), DDR&E(AC), SAE, Service Test Agencies		
<i>Background</i>	To deliver SW at speed, rigorous, automated testing processes and workflows are essential. Current DoD practices and procedures often see OT&E as a tailgate process, sequentially after development has completed, slowing down delivery of useful software to the field and leaving existing (potentially poorly performing and/or vulnerable) software in place.		
<i>Desired State</i>	Development systems, infrastructure, and practices are focused on continuous, automated testing by developers (with users) with frequency dependent on type of software, but targets cycle times measured in weeks. To the maximum extent possible, system operational testing is integrated (and automated) as part of the development cycle using data, information, and test protocols delivered as part of the development environment. Embedded software in safety-critical systems is tested with high confidence in representative (physical and simulated) environments. Testing and evaluation/certification of COTS components is done once (if justified), and then ATO reciprocity (Rec B3) is applied to enable use in other programs, as appropriate. System-level testing using modeling and simulation ("digital twin") is routinely used.		
<i>Role of Congress</i>	DOT&E should provide annual reports to Congress that describe the availability, scale, use, and effectiveness of automated T&E, with the expectation that level/depth of testing will increase at the same time as speed and cycle time are being improved.		
Draft Implementation Plan		Lead Stakeholders	Target Date
B2.1	Establish procedures for fully automated testing on digital infrastructure (Rec B1), updating DoDI 5129.47 and Service equivalents as needed.	USD(A&S), DOT&E, with Service Testers	Q1 FY20
B2.2	Establish processes for automated and red-team-based security testing, including zero-trust assumptions, penetration testing, and vulnerability scanning.	USD(A&S), DOT&E, with Service Testers	Q1 FY20
B2.3	Identify initial programs to use tools and workflows.	SAE	Q1 FY20
B2.4	Implement minimum viable product (MVP) tools and workflows on digital infrastructure (Rec B1).	SAE, DOT&E, with PMOs	Q2 FY20
B2.5	Migrate initial programs to digital infrastructure using automated T&E.	PEO, with Responsible Organizations	Q3 FY20
B2.6	Use tools and workflows, identify lessons learned and improvements (using DevSecOps iterative approach).	Service Testers, with PEO/PM	Q4 FY20

B2.7	Modify tools and workflows; document procedures.	Responsible Organizations, Service Testers	Q4 FY20
------	--	--	---------

SWAP concept paper recommendations related to this recommendation

10C	Automate testing of software to enable critical updates to be deployed in days to weeks, not months or years.
D&D	Create automated test environments to enable continuous (and secure) integration and deployment to shift testing and security left.
Visits	Automate testing of software to enable critical updates to be deployed in days to weeks, not months or years (also requires changes in testing organization).
Visits	Add testing as a service.

SWAP working group inputs (reflected in Appendix F) related to this recommendation

Acq	DOT&E should use test data collected through existing test methodologies present in software-intensive programs and not recommend or prescribe additional independent, one-time test events.
Acq	One-time IOT&Es or cybersecurity test events should not be recommended for software-intensive systems except in specific circumstances if warranted.
T&E	Build the enterprise-level digital infrastructure needed to streamline software development and testing across the full DoD software portfolio.
T&E	DoD should expand DOT&E's current capability to obtain state-of-the-art cyber capabilities on a fee-for-service basis.

Related recommendations from previous studies

DSB87	Rec 27: Each Service should provide its software Using Commands with facilities to do comprehensive operational testing and life-cycle evaluation of extensions and changes.
SEI12	Merge agile and security best practices (e.g., integrate vulnerability scans into continuous integration process, leverage automated test cases for accreditation validation, adhere to secure coding standards).
SEI16	Employ concurrent testing and continuous integration.
USDS	When issuing a solicitation, it should explain the agile software development process. The solicitation should also describe the required testing of functional requirements and make it clear that testing should be integrated into each sprint cycle.
IDA18a	Analysis of planned operational test lengths indicates that the test scope is generally not long enough, demonstrate operational reliability with statistical confidence.