



# DoD Instruction 5000.89, Test and Evaluation

- d. The **DOT&E requires** testing of cybersecurity during OT&E to include the **representative users** and an operationally representative environment. This may include **hardware; software** (including embedded software and firmware); **operators; maintainers**; operational cyber and network defense; **end users**; network and system administrators; help desk; **training; support documentation; tactics, techniques, and procedures**; cyber threats; and other systems that input or exchange information with the system under test, as applicable.
- b. DBS PMs will **develop a TEMP or other test strategy documentation**. The PM will describe the test strategy and essential elements of the TEMP in the DBS implementation plan. Specific T&E management content requirements in the implementation plan include:
  - (3) T&E planning will **include mission-oriented developmental T&E with actual operators performing end-to-end scenarios** in a controlled environment to **collect human-system interface data and reduce risk** during operational testing.
- d. ...To **maximize the benefit of early and automated data collection opportunities**, the PM must collaborate with the T&E interfaces and work through the T&E processes defined for DT&E (see Section 5) and OT&E (see Section 6) to **tailor a plan that will enable the effective and efficient execution of analysis and evaluation**, as well as the determination of test adequacy.
  - (1) Automated testing should be used at the unit level, for application programming interface and integration tests, and **to the maximum extent possible for user acceptance** and to evaluate mission effectiveness.

*DoDI 5000.89, November 18, 2020*