Joint Planning and Execution System (JPES)

The Joint Planning and Execution System (JPES) program continues Agile software development to replace the legacy Joint Operation Planning and Execution System (JOPES) program. The Joint Interoperability Test Command (JITC) conducted an early operational assessment (EOA) in October 2023 and two functional verification tests (FVTs) in December 2023 and March 2024, which gave users an opportunity to provide feedback on the effectiveness and usability of completed portions of the software development. The IOT&E previously reported as planned for 4QFY24 has been delayed to FY26 due to program delays.

SYSTEM DESCRIPTION

JPES will provide the Joint Planning and Execution Community with a web-based application on SIPRNet to create, edit, schedule, store, and query time-phased force deployment data (TPFDD) in support of joint contingency, crisis-action, and exercise planning. JPES is using an Agile software development and test approach.

The JPES Program Management Office (PMO) is continuing sustainment of the JOPES v4.5.x until JPES can be deployed to all JOPES users. Once JPES is fully fielded and provides current JOPES capabilities, JOPES is expected to be retired.

MISSION

JPES enables joint commanders to accomplish joint contingency, crisis action, and exercise planning by:

- Linking the National Command Authority to the Joint Task Force, component commanders, and Service-unique systems at lower levels of command.
- Translating policy decisions into operational plans that meet U.S. requirements to employ military forces.
- Supporting force deployment and redeployment.
- Conducting contingency and crisis action planning.

The Joint Planning and Execution Community uses the JPES portfolio to plan and execute military operations and exercises world-wide. This includes the capability to develop, refine, and maintain TPFDD, enable the identification and management of force requirements, and track the sourcing of those force requirements in accordance with the global force management and joint planning processes. The JPES portfolio provides data to and consumes data from the applicable external systems used by the U.S. Armed Forces and supported/supporting combatant commands, as well as their respective subordinate organizations.

PROGRAM

JPES is an Acquisition Category III program. The JPES PMO intends to continue development and conduct user assessments to ensure all necessary functionality meets or exceeds that of JOPES, which JPES is replacing. The JPES PMO is implementing the Development Security Operations (DevSecOps) process as part of its Agile software development framework.

» MAJOR CONTRACTORS

- ERP International, LLC – Laurel, Maryland
- NextGen Federal Systems – Morgantown, West Virginia
- Data Computer Corporation of America, Ellicott City, MD
- CompQsoft – Leesburg, Virginia

TEST ADEQUACY

JITC conducted an EOA in October 2023 and two FVT events in December 2023 and March 2024, in accordance with DOT&E's written guidance. The EOA and FVTs of JPES were conducted on SIPRNet and observed by DOT&E. The JPES integrated test environment on NIPRNet does not currently capture the differences between JPES operational environments (e.g. different commands using JPES). The JPES PMO plans for quarterly operational assessments in FY25; however, the IOT&E previously reported in DOT&E's FY23 Annual Report as planned for 4QFY24 has been delayed to FY26 due to program delays.

JPES test strategies must be developed to encompass the program's Agile nature and varying operational site requirements. The TEMP and the Agile Operational Test Plan (AOTP) are expected to be completed in FY25. The JPES TEMP should detail operational cyber survivability tests that include a cooperative vulnerability and penetration assessment (CVPA) followed by an adversarial assessment (AA).

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

JITC assessed the operational users' feedback from the EOA and FVT test events conducted in FY24. DOT&E will consider that data in the IOT&E report, expected to be released in FY26.

» SURVIVABILITY

No cyber survivability testing of JPES has been conducted. DOT&E’s FY26 IOT&E report will address findings from the planned CVPA and AA.

RECOMMENDATIONS

DISA should:

1. Improve the operational representativeness of the JPES integrated test environment to ensure testing more closely reflects the differences of the operational environments, as discussed in the FY23 Annual Report.
2. Submit a JPES TEMP and an AOTP to DOT&E for approval, as discussed in the FY23 Annual Report.
3. Conduct a CVPA and an AA during the IOT&E of JPES, as discussed in the FY23 Annual Report.