Joint Biological Tactical Detection System (JBTDS)

The Joint Biological Tactical Detection System (JBTDS) Engineering Manufacturing and Development phase testing in the DOT&E-approved Milestone B Test and Evaluation Master Plan (TEMP) is complete. Test results identified system-to-system variability in detection sensitivity attributed to degraded internal pump performance. The JBTDS collector functioned as intended and testing of the identifier demonstrated acceptable performance for most of the targets. The Program Office is working with the vendor to improve performance of the identifier assay for the remaining targets. Vendor-conducted testing of the new assays appear promising. The Program Office is working with the test community to identify and plan regression testing to verify performance improvements. The planned 4QFY22 Milestone C decision has been delayed.

SYSTEM DESCRIPTION

The JBTDS consists of an integrated man-portable biological warfare (BW) agent detector and sample collector, a base station, a meteorological station, a GPS receiver, a sample extraction kit, and a handheld BW agent identifier with consumable assays. The detector and sample collector can be connected to the base station using a Service provided, closed, or restricted local area wired or wireless network to enable remote monitoring and reporting.

MISSION

In a biological threat environment, the Army, Navy, and Marine Corps units equipped with the JBTDS will

conduct biological surveillance missions to detect the presence of, warn against, collect samples of, and provide identification of biological agents to support force protection decisions, enable medical planning, and manage consequences.

PROGRAM

The JBTDS is a joint Service Acquisition Category II program. DOT&E approved a revision to the Milestone B TEMP in November 2020. The Test and Evaluation Integrated Product Team is updating the TEMP to address regression testing. Planned Milestone C and IOT&E are expected to slip.

» MAJOR CONTRACTORS

- Chemring Sensors and Electronic Systems – Charlotte, North Carolina
- Biomeme – Philadelphia, Pennsylvania

TEST ADEQUACY

The JBTDS program conducted a shipboard operational assessment in December 2021 and completed the planned Engineering Manufacturing and Development phase integrated developmental/operational live agent chamber testing in March 2022, in accordance with the DOT&E-approved test plan. DOT&E did not observe live agent testing due to safety restrictions. Performance data from agent chamber testing was used as input for operational scenario modeling and simulation to assess the operational contribution of the JBTDS to reducing casualties resulting from a BW agent attack. The Program Office conducted false detection and identification testing in industrial, agricultural, urban, and maritime environments. Detectors were operated for 6,739 hours and 638 samples were analyzed by the JBTDS identifier. Testing was adequate to support an assessment of the current operational performance, suitability, and survivability of the JBTDS.

PERFORMANCE

» EFFECTIVENESS

During BW integrated chamber testing, the JBTDS was able to detect 60 percent of agent preparations tested at required levels. The identifier met the operational requirements for 70 percent of biological agents. The presence of battlefield interferents significantly impacted detector performance. Over the course of chamber testing, JBTDS performance degraded and system-to-system performance varied significantly. Demonstrated sample extraction efficiency was less than 25 percent for the agents tested. The Program Office is working with the vendor to identify and implement corrective actions.

Initial modeling and simulation using Service concepts of operation and test data indicates that JBTDS contributes to mitigating the effects of a BW attack. The time between an attack, detection of the attack, operational decisions to increase the force protective posture, the collection of a sample and identification of a BW agent and the use of prophylaxis to reduce casualties impacts the ability to reduce casualties.

» SUITABILITY

JBTDS demonstrated variable system-to-system detection sensitivity during BW testing caused by performance degradation of the system's internal pump. The system's built-in test capability did not alert the operator to the degraded pump performance. The vendor's investigation revealed that the JBTDS application for the pump requires operation outside its manufacturer's specifications. Navy operators expressed safety concerns regarding plans to store and charge JBTDS batteries aboard ships. The JBTDS tripod legs experienced failures after repeated set-up, stowage, and after ship shock testing. JBTDS consumables packaging resulted in the generation of burdensome waste that must be collected, stored, and disposed of in an operational environment. To date, JBTDS has not demonstrated operational suitability.

» SURVIVABILITY

The cooperative vulnerability and penetration assessment and adversarial assessment identified several vulnerabilities in a cyber-contested environment.

Test units were not able to distinguish cyberattacks from simulated biological attacks during the operational assessment. Electromagnetic interference, ship shock and vibration developmental testing resulted in JBTDS failures that need to be resolved. An electronic warfare developmental test revealed vulnerabilities in the JBTDS mesh sensor network to various threats that disrupt the ability to remotely monitor the sensor network.

RECOMMENDATIONS

The Program Office should:

1. Add built-in-test capability to alert the system operator to component failures that would negatively impact detection and sample collection performance.
2. Replace the detector collector pump to improve system performance and reliability.
3. Improve the identifier assays to meet performance requirements.
4. Address cybersecurity deficiencies to protect against cyberattacks.
5. Redesign the JBTDS legs to improve suitability and survivability aboard Navy ships.
6. Develop training to troubleshoot network issues and identify potential cyber and electronic warfare attacks to improve cyber survivability.