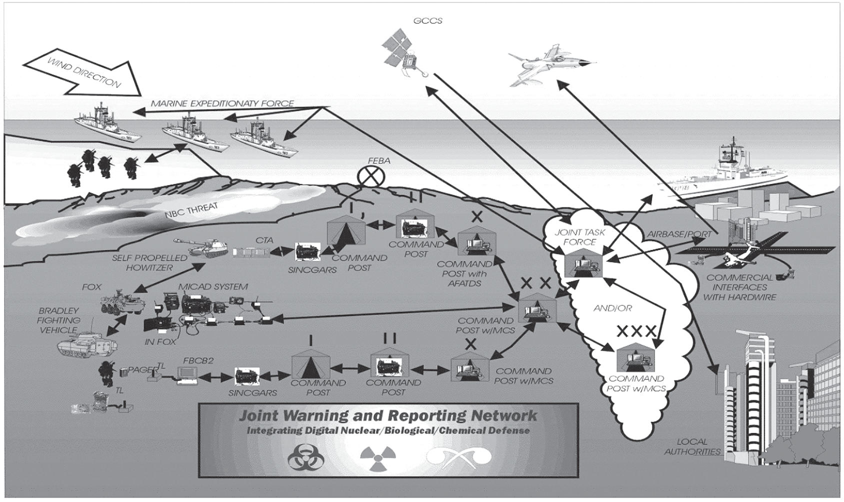
Joint Warning and Reporting Network (JWARN) Block II

SUMMARY

- The Joint Program Manager for Information Systems (JPM-IS) took control of project management for the Joint Warning and Reporting Network (JWARN) program in early July 2003.
- The JPM-IS modified the existing acquisition strategy, which the Marine Corps Systems Command had previously developed. The new strategy, approved in February 2004 by the Under Secretary of Defense, Acquisition, Technology, and Logistics, combines two block developments into one for greater capability and earlier fielding.



JWARN will collect, edit, and disseminate CBRN reports and predict downwind hazards in accordance with NATO procedures.

- The Program Manager will develop Block II in two phases, Phase 1 (B2P1) and Phase 2 (B2P2). Phase 1 is just a development stage, intended to reduce risk and streamline testing. The JPM-IS will only field Phase 2.
- The JWARN Interim Capability (JIC) is a developmental tool. The intent is to deploy it to various agencies and schoolhouses, in early FY05, to develop concept of operations and provide user feedback. The Services do not intend to field the JIC to operational forces.

SYSTEM DESCRIPTION AND MISSION

The Services intend JWARN to provide joint forces with a comprehensive analysis and response capability to minimize the effects of chemical, biological, radiological, and nuclear (CBRN) attacks, accidents, and incidents. It will provide the operational capability to employ CBRN warning technology. This technology will collect, analyze, identify, locate, report, and disseminate CBRN warnings. The JWARN will be compatible and integrated with Joint and Service-specific common and non-common operating environment-based tactical Command, Control, Computers, and Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems.

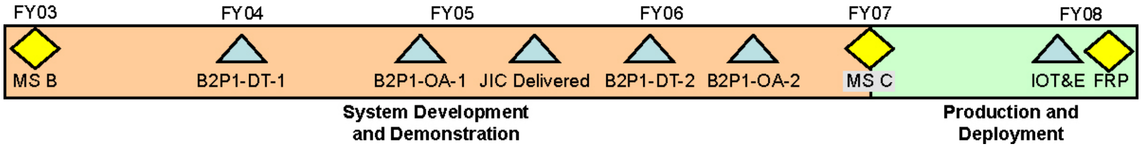
The JWARN system consists of the JWARN mission application software and an interface device.

- The mission application software will be hosted on Joint and Service Global Command and Control Systems (GCCS), and Service tactical C4ISR systems including Command and Control Personal Computer, Joint Tactical Common Operational Picture Workstation, Advanced Field Artillery Tactical Data System, Force XXI Battle Command and Control Brigade and Below.
- The JWARN Component Interface Device is a hardware device that provides connectivity between CBRN sensors and the C4ISR network.

JWARN will collect, edit, and disseminate CBRN reports and predict downwind hazards in accordance with NATO procedures.

The system will share information with the Joint Operational Effects Model, which will generate hazard prediction plots for display on operational graphics.

TEST AND EVALUATION ACTIVITY



Developmental Testing 1 (DT1), conducted in August and September 2004, focused on the B2P1 JWARN Mission Application Software and its integration with GCCS-Joint and GCCS-Maritime. It exercised the interfaces with current hazard prediction models such as Hazard Prediction and Assessment Capability. The result of this test will be available after December 2004. An operational assessment is planned in FY05 to assess the capabilities of B2P1.

The Test and Evaluation Master Plan is currently under revision to reflect the new acquisition strategy and testing guidance from DOT&E. Projected submission to the Joint Program Executive Office – Chemical/ Biological Defense is December 2004.

TEST AND EVALUATION ASSESSMENT

Timely warning and reporting within a systems-of-systems test with JWARN, the C4ISR networks, the JWARN JCID, the Joint Operational Effects Model, and CBRN sensors will be key in determining the systems' overall effectiveness and suitability.

Although the Services will not field B2P1, the JPM-IS and the contractor must maintain sound configuration control of this software. They must correct any deficiencies discovered in Developmental Testing 1 for the early operational assessment to be meaningful.

JWARN is a software system that is connected to the Global Information Grid. Operational testers must assess security measures, vulnerabilities, and Information Assurance in a robust operational environment. To this end, operational testers will use Red Teams to attempt to disrupt the system or gain access to critical operational information on the C4ISR hosts. A waiver from NATO is required in order to employ NATO Restricted AEP-45 methodology on non-NATO C4ISR networks. JPM-IS is seeking this waiver.