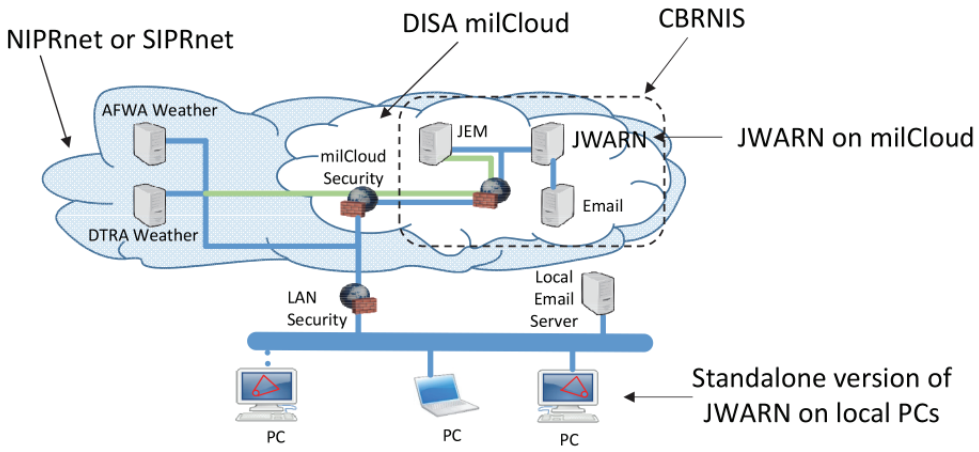
Joint Warning and Reporting Network (JWARN)

Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted operational testing of the Joint Warning and Reporting Network (JWARN) Increment 2 hosted on the Defense Information Systems Agency (DISA) Military Cloud (milCloud) between January 22, 2018, and February 3, 2018, at Eglin AFB, Florida.
- JWARN Increment 2 hosted on milCloud and standalone computers is operationally effective to support chemical, biological, radiological, and nuclear (CBRN) situational awareness and planning. Operators employing JWARN are able to provide information to support time critical operational decisions.
- JWARN Increment 2 is operationally suitable when employed in conjunction with a standalone version of JWARN for continuity of operations, and survivable in a cyber-contested environment.



AFWA - Air Force Weather Agency
CBRN - Chemical, Biological, Radiological, Nuclear
CBRNIS - CBRN Information System
DISA - Defense Intelligence Systems Agency
DTRA - Defense Threat Reduction Agency
JEM - Joint Effects Model
JWARN - Joint Warning and Reporting Network
LAN - local area network
NIPRNET - Non-classified Internet Protocol (IP) Router Network
PC - personal computer
SIPRNET - Secret Internet Protocol Router Network

System

- JWARN is a software application that integrates CBRN data into joint and Service command and control systems for battlespace situational awareness. It incorporates and displays sensor alert information and CBRN observation reports on the Common Operational Picture, and generates a warning message to units.
- JWARN replaces the manual processes of incident reporting and hazard plot generation, and warning of affected operational forces. The application is based on the standards outlined in NATO Allied Technical Publication 45, "Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological, and Nuclear Incidents (Operators Manual)."

Mission

A unit equipped with JWARN provides analysis of potential or actual CBRN hazard areas based on operational scenarios or sensor and observer reports, identifies affected units and operating areas, and provides warning information to support commanders' force protection and operational decisions.

Major Contractor

Northrop Grumman Mission Systems – Orlando, Florida

Activity

- AFOTEC conducted initial operational testing of JWARN Increment 2 on the DISA milCloud and local computers from January 22, 2018, to February 3, 2018, at Eglin AFB, Florida. The Army Threat Systems Management Office conducted an Adversarial Assessment during the operational test.
- AFOTEC conducted the operational test in accordance with the DOT&E-approved test plan. The test was adequate to assess the operational effectiveness, operational suitability, and cybersecurity of JWARN hosted on milCloud and the continuity of operations plan associated with the use of JWARN Increment 2 operating on a local computer.
- The Joint Program Executive Office for Chemical, Biological, Radiological, and Nuclear Defense authorized full deployment of JWARN Increment 2 Requirements Definition Package-2 Capability Drop 2.1 on milCloud on August 17, 2018.

Assessment

- JWARN Increment 2 hosted on milCloud is operationally effective to support CBRN situational awareness to support operational decision-making and planning.
- JWARN Increment 2 met and in some cases exceeded the operational requirement for timely warning of downwind units at risk.
- JWARN Increment 2 is operationally suitable when employed in conjunction with a standalone version of JWARN for continuity of operations. JWARN demonstrated the required 96 percent probability of successful mission completion for warning and reporting missions.
- JWARN is survivable against cyber-attacks. Hostile cyber activity during testing had no significant effect on the unit equipped with JWARN ability to accomplish its mission.

Recommendations

None.