

FACT SHEET

www.cwid.js.mil



Coalition Warrior Interoperability Demonstration

CONTACT CWID Joint Management Office Public Affairs at 757-225-2172 or CWIDPA@langley.af.mil
2101 Executive Drive, Hampton, Virginia 23666

CWID 2010 OBJECTIVES

Coalition Warrior Interoperability Demonstration (CWID) engages U.S. Combatant Commands, Coalition Partners, U.S. Military Services, DOD Agencies, and Homeland Security/Homeland Defense (HS/HD) organizations to identify capability shortfalls for technologies to fill each year. Using a simulated operational scenario, warfighters and operators assess each technology for operational utility while technical experts evaluate technical interoperability and the ability to provide information assurance.

1. Improve Coalition Command, Control and Coordination in Conventional and Irregular Warfare Operations

- a. Demonstrate real time, beyond line-of-sight / while on-the-move, C2 coordination and situational awareness
- b. Demonstrate real time voice and text translation
- c. Demonstrate multi-domain applications that promote secure, seamless information sharing with mission partners
- d. Demonstrate information exchange and interoperability capabilities between military and civil authorities at the Federal, State, and Local levels
- e. Demonstrate command decision support tools for processes at the strategic and operational levels

2. Improve Leader Centric, Net-Enabled Operations

- a. Demonstrate bandwidth optimization and quality of service management tools
- b. Demonstrate effective network defense applications to protect shared data being processed, in-transit and/or at-rest
- c. Demonstrate a secure, deployable / modular network capability to enable dispersed operations over "open" networks
- d. Demonstrate data fusion tools, using a service oriented architecture, that operates and maintains C/C/S/A C2 capabilities while leveraging respective core competencies
- e. Demonstrate tools to transition the GCCS family of systems to Net-enabled C2 (NECC)
- f. Demonstrate technologies to efficiently direct, task and manage the intelligence process

3. Enhance Coalition Battle Space Situational Awareness

- a. Demonstrate interoperability of biometric capabilities
- b. Demonstrate secure information exchange capabilities that enhance worldwide maritime, land and air domain awareness among joint forces, coalitions and agencies
- c. Demonstrate improved blue force tracking, identification and engagement management capability
- d. Demonstrate ISR data visibility, engagement and database synchronization perimeter defense tools to include near real-time engagement capability
- e. Demonstrate the interoperability of Multilateral Interoperability Program (MIP) compliant mission planning coordination and awareness tools

4. Enhance Coalition Logistics Planning and Coordination

- a. Demonstrate logistics data access, synchronization and display of secure, real-time status / location of resources
- b. Demonstrate tactical level logistics originating from a sea-base concept in support of operations ashore
- c. Demonstrate secure, large medical and health protective services file data sharing and analysis capability, (e.g. would be associated with Pandemic Influenza planning)
- d. Demonstrate the capability to plan and coordinate logistics operations between US, NATO and other coalition forces

5. Enhance Coalition, Military, Government Agency, International Organization and NGO Partnership Building Capabilities

- a. Demonstrate cyberspace surveillance and computer network defense capabilities
- b. Demonstrate tactical level IA and data sharing between DoD, GOs, NGOs and coalition partners
- c. Demonstrate unclassified, COP visualization technologies between military, GOs, NGOs, and coalition partners
- d. Demonstrate a blue force tracking capability or application for 1st responders
- e. Demonstrate communication tools that share Defense Support to Civil Authorities (DSCA) data access, fusion & integration with DoD
- f. Demonstrate mission planning and readiness management tools that support DoD, GOs, NGOs, law enforcement and 1st responders

6. Improve Secure Information Sharing Between Disparate Security Domains and Communities of Interest in an Operational Environment

- a. Demonstrate the capability to securely subscribe to a data feed originating in another domain and to automatically distribute data back into the requesting domain
- b. Demonstrate the capability to provide visibility of global address lists and to securely exchange emails containing attachments between consumers located within and between multiple security domains
- c. Demonstrate enhanced multi-media / digital data streaming (e.g. audio & full motion video) across multiple domains
- d. Demonstrate the capability to provide identification & authentication credentials and attributes across multiple domains
- e. Demonstrate chat and dynamic session establishment capabilities with multiple consumers located across multiple domains
- f. Demonstrate the capability to post data to a repository in one domain while enabling secure access to/from consumers in another
- g. Demonstrate the capability to audio conference across multiple domains
- h. Demonstrate the capability to perform centralized network monitoring that provides functional visibility, secure remote access and status reporting for all domains
- i. Demonstrate the capability for cross domain mission information discovery

7. Improve Centralized Command, Decentralized Control for Irregular/Hybrid Warfare Units

- a. Demonstrate technologies to enhance highly specialized small units operating in a dispersed manner
- b. Demonstrate technologies to fuse and correlate disparate ISR data at the tactical level
- c. Demonstrate technologies that provide integrated and multi-layered security C2 capabilities with other agencies, and nations

#

(CURRENT AS OF March 2010)