

"[AWS] is very critical to our operations, people want to know if oil is going to spread to port facilities."

USCG Lt. Cmdr. Ted Kim

USCG's IP-Based AWS 2.0 Supports Deepwater Horizon Response

BY STEVEN TITCH ON JUNE 4, 2010

Network-centric mass notification has taken a major role in emergency maritime communications surrounding the BP Deepwater Horizon disaster in the Gulf of Mexico.

The U.S. Coast Guard has been using its Alert and Warning System (AWS) 2.0 to keep Coast Guard, industry and civilian personnel updated on port and waterway closings and other effects the April 20 underwater well explosion—and ongoing repair efforts—have had on ship traffic. Since the explosion, the oil spill has been spreading from its source about 40 miles off the southeast coast of Louisiana and has been defying efforts to contain it.

"[AWS] is very critical to our operations," said USCG Lt. Cmdr. Ted Kim. "People want to know if oil is going to spread to port facilities."

As of this week, the Coast Guard had issued 13 messages that have been received by some 4500 internal and external users, Kim said. Internal users describe Coast Guard officials. External describes industrial and civilian users. Examples include a May 10 message sent to internal and external users that Port Fourchon, located along the southern tip of Louisiana, was open, correcting misinformation in earlier reports. Not all reports were confined to the Gulf Coast region. On May 23, internal notification was sent to Sector Honolulu requesting additional personnel for the Gulf, Kim said. The Coast Guard's Sector Mobile (Ala.) also used the AWS system to postpone a search-and-rescue exercise that had been scheduled for Gulf waters near the spill, he added.

AWS 2.0 uses email, landline, wireless, satellite, fax and text messaging to transmit alerts and messages to Coast Guard personnel, port officials and thousands of civilian vessel operators on natural disasters, hurricane preparedness, search and rescue operations, and waterway closures. Set up under the Maritime Transportation Security Act of 2002, the AWS 2.0 upgrade represents an embrace of network-centric security and emergency communications systems. The centralized server-based system, which cut over late last year, replaced a cumbersome emergency notification process that depended on a string of actions local level, often without central coordination. It also will improve the Coast Guard's ability to account for the reception of messages and alerts by taking advantage of the way IP-based services such as email and text messaging permit immediate reply.

The system uses an IWSAlerts platform from AtHoc Inc., and encompasses more than 100 USCG facilities, from headquarters down to district, sector and local stations. It has the capability to reach 50,000 USCG personnel and maritime industry members from Maine to Hawaii.

For Kim, the AWS communications system, managed out of Martinsburg, W.Va., is part of a larger effort "From my point of view, we've been doing a lot of IT support for Deepwater Horizon [response]," he said. That effort that extends to the Coast Guard's Homeport website, which links to the official Deepwater Horizon Response site. "In every aspect here, we're trying to provide the IT support to make [responders'] jobs easier."