



Federal Computer Week

## NMCI grows despite delays

BY [Matthew French](#)  
Aug. 26, 2003

Printing? Use this [version](#).

[Email](#) this to a friend.

The Navy Marine Corps Intranet is now the largest network in the Navy. With more than 95,000 seats cut over, the enterprisewide network is about one-third complete, despite delays caused by massive numbers of sailors and Marines deployed overseas.

One particularly difficult task has been readying the Marines' network operations center in Quantico, Va., because of the lack of an adequate infrastructure and enough Marines to begin using the network, said Navy Capt. Chris Christopher, NMCI's staff director.

The center will be located in a temporary facility at Quantico until a permanent building can be found or constructed. The Marine Corps is scheduled to cut over to NMCI in October and November, regardless of whether or not the Marines have returned from serving abroad. The center will be up and running by mid-September, said an NMCI spokesperson.

"A big chunk of the Marine Corps has deployed, and that has affected the schedule of the Marine Corps' rollout," Christopher said. "There was no catastrophic effect, but it did have an impact."

Next on the NMCI schedule is an evaluation that will take place in early October. It will closely examine the deployment and operation of the network. "We would like to see issues raised at the last operational evaluation successfully addressed," Christopher said. "Last year, the evaluation involved about 20,000 seats; this year, we'll have more than 100,000."

The Navy is also progressing to reduce the great number of legacy applications that have slowed NMCI's rollout.

Advertisement

Protocol  
Anomaly  
Detection  
Identifies  
both known  
and unknown  
attacks

### RELATED LINKS

[Navy's Navy Marine Corps Intranet Site](#)

["Navy steadily reducing legacy apps"](#) [FCW.com, June 18, 2003]

["Navy labors over legacy systems"](#) [FCW.com, March 19, 2003]

["New Army CIO to deal with legacy"](#) [FCW.com, May 28, 2003]



The Navy has been developing a list of 2,000 to 3,000 core applications that everyone in the Navy and Marine Corps will use when NMCI is up and running. Functional area managers -- those responsible for specific functions, networks and applications in NMCI -- have been developing lists of approved applications that will make the transition from their stand-alone environment to NMCI.

Some applications not on the list are approved for use if the local commander can prove they are necessary, which often leads to service members working on two workstations at the same desk. That ends Oct. 1, Christopher said.

The actual elimination of the applications will take a few years. Getting the list in place is an important first step.

To assist in reducing legacy applications and identifying which systems comply with NMCI's security policies, the Navy announced a two-year, \$5.8 million deal with Securify Inc.

Under terms of the contract, EDS, the lead contractor on the NMCI project, will deploy Securify's SecurVantage security management products to determine if legacy systems comply with the more stringent NMCI security policies.

"As the Navy moves more and more from its 'as is' legacy systems to the 'to be' NMCI systems, there are a lot of challenges that are arising," said Carl Wright, Securify's vice president of federal operations, "and most of those are centered around legacy applications."

Applications are being eliminated outright, scaled back or integrated into the NMCI environment throughout the Navy. Those that will be included in the NMCI environment must pass certification tests to determine if they comply with NMCI regulations.

"When you connect legacy networks [to NMCI], there is a certain level of uncertainty," Christopher said. "Securify will help the network administrators understand what traffic is flowing through their networks."

This type of security exists within the NMCI environment, he said, but is lacking in the less secure legacy networks. Before the transition to NMCI can take place, administrators need to have a more comprehensive idea of what their networks are doing and if they comply with NMCI's security policies.