

Hamre “Cuts” Op Center Ribbon, Thanks Cyberwarriors

JIM GARAMONE

ARLINGTON, Va. —Deputy Defense Secretary John Hamre presided over an Aug. 11 “virtual” ribbon-cutting ceremony here officially opening the Joint Task Force (JTF) — Computer Network Defense Operations Center.

The JTF, located at the headquarters of the Defense Information Systems Agency, is the focal point for defense of DoD computer systems and networks. Hamre called the task force an investment America must make.

“Several times I’ve testified and talked on Capitol Hill about the future electronic Pearl Harbor that might happen to the United States,” Hamre told the standing room only crowd. “I’ve used that expression not to talk about surprise attacks. ... The most important message about Pearl Harbor was the way in which we had actually prepared well in advance for the war that came.”

He said the designs for the capital ships the Navy used during World War II were finished before Dec. 7, 1941. Most of the designs for Army Air Forces combat aircraft were also finished before America entered the war.

“They had the foresight to see [the war] coming and do something about it,” Hamre said. “That really was the message of Pearl Harbor. It wasn’t that we got hit. It was that we were ready to respond.”

That’s what drives the task force — DoD is not just about fighting America’s battles now, but also those in the future.

“It’s buying the infrastructure, in advance, that we know we are going to need at some point in time,” he said.

“It’s [about] building the infrastructure and the resources, the talents and the skills.

It’s about growing that human resource needed for when that next Pearl Harbor comes.”



Hamre said defending DoD’s computer systems and networks is “stretching everyone’s imagination.” The task force achieved initial operating capacity on Dec. 30, 1998, and full operating capacity on June 30, 1999. Establishing the office has not been easy, he noted, because the personnel had to start up while at the same time, fight a cyberwar. “[DoD] has been at cyberwar for the last half a year,” Hamre said. “At least we have a place now that can do something about it.”

Air Force Maj. Gen. John H. Campbell, task force commander, said his organization brings an operator’s eye to the table. His staff, he said, can assess what an attack is doing to a system and can tell what effect the attack would have on operations.

“The JTF is the first DoD-wide organization that can actually direct the military services to take actions to defend DoD systems and networks,” Campbell said.

DoD officials have said 80-to-100 computer "events" occur daily in Department systems. Of these, about 10 require further analysis.

To date, DoD officials have no knowledge of a breach of a classified system. But the JTF is running into increasingly sophisticated attackers. Officials believe the technology for detecting and tracking violators is keeping up with the attackers.

"DoD has come a long way, and the joint task force has given DoD a mechanism that allows more coordination between the Services and Agencies that just didn't exist before," said JTF spokesperson Melissa Bohan. "The JTF ... looks across the Department and monitors computer incidents. However, this is an area for continuing research and development."

The Joint Task Force - Computer Network Defense has already made itself felt throughout DoD. It recently issued a directive instructing all the Services and other DoD organizations to complete a number of actions to improve network and system security. The actions included changing administrative

and user passwords and then restarting operating systems with a "warm boot" — like using a home computer's "reset" button rather than its on-off switch.

"DoD organizations are implementing this advisory as their own management deems appropriate," Bohan said. "The JTF's Service components and the Defense Information Systems Agency's DoD Computer Emergency Response Team, and other nonintelligence DoD agencies, must comply. For the intelligence-based DoD agencies and the commanders-in-chief, this message was for coordination and information only. The change is still ongoing."

Hamre said all of DoD must become more concerned about computer security, and he thanked the members of the Joint Task Force for their efforts. "When [cyberwar] becomes really serious, the Department will be ready, thanks to your efforts," Hamre said.

Editor's Note: This information is in the public domain at <http://www.defenselink.mil/news>.