DOD reels in content on Web sites

By Bob Brewin, Dan Verton, L. Scott Tillett, L. Scott Tillett | Sep 20, 1998

Concerned about the security risks posed by the availability of some types of information on the World Wide Web, the Defense Department has begun to pull pages from its Web sites while top DOD officials carry out a department-wide review.

At the direction of the Joint Staff, the Defense Information Systems Agency recently removed links to detailed architectural information on the Global Command and Control System, according to a note posted on DISA's Web site.

Deputy Secretary of Defense John Hamre and the Joint Staff are concerned that terrorists and other hostile forces might be able to glean revealing and damaging information on U.S. forces from the department's estimated 1,000 Web sites. Hamre and department leadership are considering a "tasking memo," which would fine-tune procedures for maintaining information on DOD Web sites, based on a depart-mentwide review of its sites.

Marv Langston, DOD's deputy chief information officer, said concerns about terrorist exploitation of freely available information has forced the Pentagon to re-examine its Web policies. "We want to make sure we don't harm ourselves, but we also want to keep things open for the sake of efficiency," Langston said.

Inadvertent release of sensitive information on Web sites reflect what Langston termed "the age-old debate" of how to handle sensitive information in an open society. "We don't want to overreact, but we also don't want to underreact," he said.

A knowledgeable industry source with strong ties to DOD command, control and communications communities said the concerns about the types of information available on unclassified DOD Web sites surfaced earlier this summer, well before the terrorist attacks on embassies in Tanzania and Kenya.

The source said the annual "Evident Surprise" information warfare exercise, which was conducted by the U.S. Atlantic Command, headquartered in Norfolk, Va., showed top DOD officials "how much unclassified information that was available [on the Web] could be used to attack the U.S. military."

Officials from the command have repeatedly sidestepped requests for the release of any information on Evident Surprise throughout the summer, citing security issues. But sources said the exercise showed easily exploitable holes in DOD systems and in information systems operated by private-sector participants, including commercial utility companies.

The danger stems from certain types of sensitive data and from the aggregate of seemingly harmless information, DOD sources said.

"Obviously you can take a hell of a lot of stuff and drive something by putting it together," said Kurt Molholm, administrator of the Defense Technical Information Center, which oversees about 90 Web sites. "Seventeen hundred different innocuous" pieces of information could be dangerous once pieced together, he said.

Hamre and the Joint Staff are reviewing the content of DOD Web sites to see what sort of information they may provide, a Pentagon spokesman said.

review the Web sites with a couple of basic principles that deal with personal and other types of security and to make sure that they don't give out information that could compromise our very legitimate security needs," the spokesman said.

Some of the information found on DOD Web sites "is personal information, such as Social Security numbers, home addresses, telephone numbers [and] home telephone numbers," the spokesman said. In other cases, the information deals "with very specific information about the capabilities of weapons...[and information]...that might provide very detailed floor plans of...certain types of facilities," he said.

In part, the problem stems from DOD's decentralized approach to Web site management, observers said. DOD allows each organization to decide what information to release online, just as it does with paper-based information, Molholm said.

Generally, an organization first checks to see whether the information is classified and then passes it to a public affairs office to see if the information contains material on intellectual property or other sensitive data. If the information gets the nod from public affairs officials, it goes to the Web for the world to see, Molholm said.

Jackie Devine, chief of community relations for the Air Mobility Command at Scott Air Force Base, Ill., said AMC attempts to take "the high road" by not posting pages that require passwords or that restrict access. "We steer away from operational information [and] try to make [our Web site] the lowest common denominator of public information," Devine said.

Marine Corps spokesman Capt. Mike Neumann said the Corps expects the Hamre directive to come down next week, but he added that the service already has begun an informal review of Web content on its own.

Robert Steele, chief executive officer of information consulting firm Open Source Solutions Inc., Fairfax, Va., called DOD's Internet planning problem

and it has been very slow to convert its legacy systems into Internet, Web-like interfaces."

As a result, individual services and divisions of DOD put up their own Web sites with no central coordination from DOD, he said.

John Pike, a defense analyst with the Federation of American Scientists, said he is "extremely concerned" with talk of scrubbing Defense Web sites. "My view, though, is that if it is unclassified and if it is not Privacy Act Information...it should be available online."

NEW FROM FCW

ODNI shakes up cyber structure

DIU chief: Earnings focus thwarts innovation

FAA names drone remote ID tech contractors

House bill would protect unused leave during COVID-19

New AWS protest spawns JEDI blog wars

MOST POPULAR ARTICLES

ODNI shakes up cyber structure

DIU chief: Earnings focus thwarts innovation

PPE acquisition used as bait in global phishing scheme

FCW Insider: May 7

MORE FROM PUBLIC SECTOR 360

Defense Systems

DOD tech leaders look to tune out Ligado

U.S. drone developers feel squeeze during pandemic

DISA wants to scale web-browsing protection pilot

Federal Soup

Rep. proposes feds keep leave that went unused due to pandemic

Lawmaker aims to crack down on reliance on acting officials

VA adds new 'coach' to mobile app lineup

GCN

Could 5G cause GPS problems?

Millions of products have been 3D printed for the coronavirus pandemic – but they bring risks

IT responders keep government at work

Washington Technology

These deals show some not halting their M&A plans

PAE sees COVID economic stimulus 'trickle down' effect on government services

How is the private sector pivoting to 'distance work?'