



DOD: Controlled but unclassified data is leaking

By [Alice Lipowicz](#)

Published on October 27, 2008

Controlled but unclassified Defense Department information is leaking to the public from thousands of Web sites sponsored by DOD, according to a recent memo by DOD Chief Information Officer John Grimes.

In the memo, Grimes emphasizes the importance of protecting controlled unclassified information, especially in systems that are connected to the Internet with insecure protocols such as File Transfer Protocol or Peer-to-Peer sharing.

“The Department of Defense is currently hosting thousands of such sites, and in spite of previous direction, Controlled Unclassified Information data is still publicly accessible from these Defense Department sites,” Grimes wrote in the memo, which was published by the Federation of American Scientists on Oct. 22.

Military officials have become increasingly concerned about the risks of failing to protect controlled unclassified information that may compromise battlefield strategies and technology. Some of that information is being put at risk by defense contractors, according to another document released by the federation.

In a three-page white paper, Army officials note that increasing digitization of information has lead to greater risks about leaks of information to global enemies. The white paper is marked “For Official Use Only” and was published on the Web on Oct. 22 by the scientists group.

“Simply stated, hostile actors can exfiltrate large volumes of unclassified program information in a single attack that can potentially net enough information to enable adversaries to narrow a capability gap,” the Army paper states.

“Exfiltrations of unclassified data from Defense Industrial Base unclassified systems have occurred and continue to occur, potentially undermining and even neutralizing the technological advantage and combat effectiveness of the future force,” the paper said.

The Army has established a Defense Industrial Base Cyber Security Task Force to coordinate activities to mitigate the risks, including setting up a cybersecurity acquisition initiative with the Office of the Secretary of Defense; running a pilot program to conduct damage assessments from hacker intrusions, and working with the secretary’s office to develop policies to further mitigate risk.

The policies will focus on companies in the areas of command and control; communications, intelligence, surveillance and reconnaissance; programs that affect modernization of systems; and programs that affect the security of systems for Army research, development and testing facilities, program offices and supply chains, the paper said.

© 1996-2008 1105 Media, Inc. All Rights Reserved.

<http://www.fcw.com/online/news/154195-1.html?type=pf>