

Defense networks breach reveals weaknesses in federal info security

By [Jill R. Aitoro](#) 05/14/09

Tighter information security controls on government computers could have prevented the leak of confidential documents by a Pentagon official to a Chinese operative, according to members of the security industry.

"There should be controls in place on these systems to limit copying of classified information, and logs should be reviewed regularly per employee activities on these systems," said Tom Kellermann, vice president of security awareness at Core Security Technologies and former senior data risk management specialist for the World Bank treasury security team.

James Wilbur Fondren Jr., deputy director of the U.S. Pacific Command's Washington liaison office, was charged with espionage conspiracy, according to a [May 13 press release](#) from the Justice Department. Fondren, who is on administrative leave from his job, is accused of providing an operative of the Chinese government with Defense Department documents and other information, some of which Fondren obtained from classified online systems. Fondren had Top Secret clearance and worked from both a classified and unclassified computer at his cubicle.

"The U.S. government places considerable trust in those given access to classified information, and we are committed to prosecuting those who abuse that trust," said Dana Boente, acting U.S. attorney for the Eastern District of Virginia.

In March, federal prosecutors [charged](#) a former Internal Revenue Service employee with illegally accessing agency computers and filing false claims against the government.

Many employees will do nefarious things for the right sum of money -- a fact that agencies must consider when developing strategies to protect sensitive information, said Rob Grapes, chief technologist for Cloakware, a security software vendor.

"A huge amount of money and energy is put toward perimeter protection -- protecting information from the outside in," he said. "But there's this other realm of insider threats, [stemming] from the fact that employees can quickly and easily access this information. The insider has the time and opportunity to create more significant damage to an organization. We need to look at additional security mechanisms."

Specifically, Grapes said agencies should consider partitioning information in a document -- separating the content -- so no one person will have the complete version, but only the pieces of data they need to perform their jobs. Agencies also should encrypt data, implement strict controls over access to information and the applications housing that information, and recertify at least monthly authorization rights for users. Agencies also could require dual authorization on sensitive documents, Grapes said, so no one can access the information without the knowledge and approval from another.

"That provides an auditing trail and an opportunity to deny access" if requested access is deemed suspicious, he

said.

In Fondren's case, Justice alleged that he gave the Chinese operative "opinion papers," eight of which contained classified and unclassified documents, including information about military meetings between the United States and China and a 2008 draft copy of U.S. military strategy. Both Kellermann and Grapes said such access would have raised red flags in the Pentagon if the right security controls were in place.

An effort under former President George W. Bush's largely classified Comprehensive National Cybersecurity Initiative seeks to pinpoint safety controls to improve federal information security. The National Cyber Leap Year Initiative will identify the most promising ideas from industry for reducing vulnerabilities to cyberattacks and for developing innovative, multidisciplinary security efforts.

The Leap Year initiative will run through fiscal 2009 and will define technology solutions that can help federal agencies stay ahead of any cyber threats, technical strategies for research and development, details on delivering and using capabilities, and recommendations on funding, policies and oversight.

The deadline for submitting comments on the National Cyber Leap Year initiative was April 15.

COMMENT ON THIS ARTICLE IN THE FORUM

© 2009 BY NATIONAL JOURNAL GROUP, INC. ALL RIGHTS RESERVED