

# Electronic Document Security



To subscribe or unsubscribe from this newsletter, send email to:  
Ronald.Hackett@ManTech.com

ManTech SRS Technologies, Inc.  
Systems Solutions Division  
500 Discovery Drive Huntsville, AL 35806  
Copyright © 2007  
ManTech SRS Technologies

## Sensitive Online Military Files Unprotected

A July 12, 2007, Associated Press (AP) article reported that sensitive military documents are often posted to public websites by mistake. The information is freely available to everyone via the Internet. Much of this sensitive information poses a direct threat to our troops if it were to fall into the wrong hands.



The AP reported finding dozens of sensitive documents carelessly posted to government websites—documents the government refused to release directly because of the risk to troop security. In at least one case, the AP deleted information at the government's request, only to find updated versions of the documents posted on the agency's website just a few days later.

Los Alamos National Laboratory was also cited in the AP report for documents carelessly posted to an FTP site, and the National Geospatial Intelligence Center said they were going to review their website procedures after the AP discovered sensitive documents that included aerial surveys of military airfields in Iraq.

None of these problems are new. They are all caused by the lack of adequate review procedures. None of this information was hidden in a classical sense. It was simply overlooked by the individual posting the information. Reviewers tend to focus on the information that needs to be published and overlook other data that should be excluded.

ManTech International Corporation's Document Detective could have prevented all of these unfortunate incidents. While it was originally designed to expose information hidden deep within electronic documents, Document Detective's regular expression keyword scanner can locate sensitive information anywhere within the document, including the visible information. Document Detective can locate sensitive keywords and structured data, like social security numbers. A thorough review is needed before any information is posted to the web. Document Detective automates good review practices and ensures a thorough review is conducted.

<http://www.military.com/NewsContent/0,13319,142101,00.html?ESRC=topstories.RSS>

## Secret Iraq Documents Found

Pete Moore, a political scientist, reported finding dozens of Microsoft Word documents with sensitive information hidden in the tracked changes posted in the online archives of the Coalition Provisional Authority that governed Iraq immediately after the war. In a salon.com article entitled, "The secret Iraq documents my 8-year-old found," Moore reported that 20 of the 42 documents he downloaded from the website had tracked changes.

This is yet another example of the Microsoft Ad Hoc Review feature in action. The Ad Hoc Review automatically enables tracked changes without warning when a Word, PowerPoint, or Excel file is attached to an Outlook email. The high percentage of documents with tracked changes is not

August 13, 2007

**ManTech**  
International Corporation

Leading the Convergence of National Security and Technology™



surprising, because Outlook has become the standard email client for the U.S. government. We downloaded the document mentioned in this article and found it was in a nested Ad Hoc Review cycle, and it clearly displayed the Reply with Changes button. Any Word, PowerPoint, or Excel document that displays a Reply with Changes button is in an active Ad Hoc Review cycle and is actively tracking all changes made to the document.

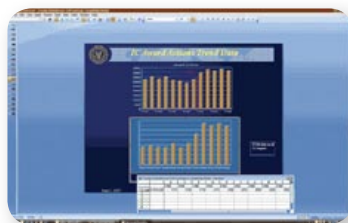
Security incidents involving tracked changes in Word are common in the press, because many people know about this feature, and because Microsoft Office 2003 displays the tracked changes in Word by default. Tracked changes in PowerPoint and Excel are not well known, and they are not easy to find in any version of Office.

Microsoft did remove the ad hoc review feature from Office 2007, but that won't do much about the millions of electronic documents already in circulation with sensitive information hidden in the tracked changes. Document Detective is the only software available that can identify and remove the Ad Hoc Review and Tracked Changes from all Microsoft Office documents. Even Microsoft's free Remove Hidden Data plug-in fails to remove the tracked changes from PowerPoint presentations.

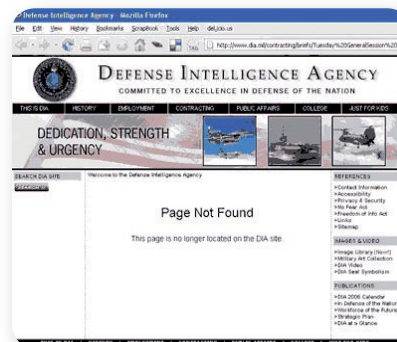
[http://www.salon.com/news/feature/2007/05/18/cpa\\_documents/](http://www.salon.com/news/feature/2007/05/18/cpa_documents/)

### DIA Exposes Classified Intelligence Budget

In a classic case of an embedded Microsoft Object Linking and Embedding (OLE) object, the Defense Intelligence Agency inadvertently exposed the magnitude of the classified portion of the Intelligence budget in a PowerPoint presentation posted to the Agency website. R. J. Hillhouse reported the incident on her website, "The Spy Who Billed Me," on June 3, 2007.



The sensitive information was contained in several Microsoft Graph Chart objects, which are similar to Microsoft Excel, but can not stand alone as separate files. Both types of embedded objects are based on Microsoft's OLE standard, which allows the data from one application to be embedded into a different application. Embedded OLE objects can contain many layers of data that are not displayed in the host application. Each embedded OLE object is a complete copy of the original file, but only a fraction of the data is displayed.



The Director of National Intelligence quickly announced that the information in the presentation was not sensitive because it was only a "draft," but the presentation was quickly removed from the website.

Once again, good review practices could have prevented this inadvertent release of sensitive information, but removing hidden data before the review would speed up the review process. Document Detective's content control toolbars allow a user to "flatten" a document. This process removes most of the hidden data quickly and easily. Combined with the content browser, Document Detective provides unbeatable information security when sharing electronic documents.

[http://www.thespywhobilledme.com/the\\_spy\\_who\\_billed\\_me/2007/06/update\\_dni\\_inad.html](http://www.thespywhobilledme.com/the_spy_who_billed_me/2007/06/update_dni_inad.html)

### Louisiana University System Leaks Personal Information

Tim Wilson, the editor for the Dark Reading website, reports that the Louisiana University System has the personally identifiable information for 80,000 employees and students posted on unprotected websites. A university student found the information, which included names, addresses, social security numbers, and other sensitive

personal information, using the Google search engine. Both the FBI and the Board of Regents is investigating the report.

Aaron Titus found over 150 electronic data files containing personal information to make a point about privacy. He reported his results on a local television station.



According to the report, the information was located on an "internal" website, but the internal website was clearly visible from the Internet, because it was located using Google.

The Louisiana State Constitution guarantees the right to privacy, according to Law professor Julian Murray, who was quoted in the television report. This incident leaves the Board of Regents open to both civil and criminal action, including the possibility of a class action lawsuit by those affected by the data leak.

This story shows how difficult it is to protect sensitive information. One mistake, like forgetting to password-protect a section of the "internal" website, can expose the data to the open Internet. One thing users can do to minimize the threat is to minimize the sensitive information in their electronic data files. Many of the data files found in the Louisiana University System website were probably unnecessary or out-dated and no longer needed. The first step in protecting sensitive data is being aware of its presence. Document Detective's regular expression keyword scanner can help identify sensitive information, including both plainly visible information and information that has been inadvertently hidden through multiple edits and pasting. Protecting sensitive information begins with the user who has access to the information and a legitimate need to use and share that information.

[http://www.darkreading.com/document.asp?doc\\_id=129381&WT.svl=news1\\_4](http://www.darkreading.com/document.asp?doc_id=129381&WT.svl=news1_4)

## Other File Formats Compromise Security

It's easy to point fingers at Microsoft because of the many security problems in their popular Office



file formats, but many other file formats can compromise security. Software developers often overlook the security aspects of embedding hidden information, and they often fail to consider how a feature can be misused for malicious purposes. We found two interesting examples of this since our last newsletter. Document Detective does not currently address these file types. We include this information to enhance your appreciation for the magnitude of the hidden data threat.

Robert Jaques reported on vnunet.com that a new OpenOffice macro worm called BadBunny-A had been discovered. This macro worm downloads a picture of a man dressed in a bunny suit performing indecent acts in the woods with a scantily clad woman. The worm is not specific to a single operating system, and contains attacks for Windows, Linux, and MacOS.

<http://www.vnunet.com/vnunet/news/2190354/openoffice-worm-downloads-bunny>

Dave Zeiler reported in the Baltimore Sun, June 7, 2007, that Apple has been embedding personal information in their popular iTunes files. The information, which has been embedded since the original iTunes launched in 2003, is easy to recover using the Get Info command. In an interview with Wired magazine, industry analyst Mike Gartenberg said, "The information could be used as a proof of purchase, or to facilitate upgrades," in addition to fighting piracy. While this seems like a valid use, Wired magazine questioned why the information was not encrypted or protected.



<http://www.baltimoresun.com/technology/bal-bz.pl.apple07jun07,0,7819604.story?coll=bal-technology-headlines>

## **ManTech International Acquires SRS Technologies and Document Detective**

ManTech International Corporation, a leading provider of innovative technologies and solutions for mission critical national security programs, acquired SRS Technologies on May 8, 2007. ManTech strongly supports Document Detective, and we look forward to enhancing their mission to provide the very best in security. For additional information on the merger, go to: <http://www.mantech.com>.

Document Detective developers routinely run evaluations on real documents found on the Internet as part of our test program. Last month, we discovered a highly classified, special compartmented information presentation hidden in the tracked changes of an unclassified PowerPoint presentation transmitted via the Internet. This incident demonstrates that hidden data in electronic documents is a real and significant threat. We contacted the organization responsible and helped them clean up the problem.

A new version of Document Detective will be released this fall. This version will enhance our font parameter testing, especially in Microsoft Word. Many "metadata" programs identify four font conditions that could obscure text, but Document Detective will detect 12 font conditions that could obscure text. Enhancements to the review certificate



will allow for multiple reviewers, and the new version of Document Detective can post the reviewed documents to a transfer agent server currently in development. The transfer agent is a bridge between the rigorous review process provided by Document Detective and an approved transfer process, such as a secure guard. The transfer agent makes a completely automated, electronic cross domain solution possible.

ManTech SRS Technologies is committed to continuing research and product development in the area of electronic document security. While no process or procedure is perfect, Document Detective is an ideal solution for reviewing and sanitizing electronic documents, especially when national security information is at stake.

Please feel free to share this newsletter with anyone you believe would benefit from this information.

This newsletter is dedicated to raising awareness about the Desktop Publishing Threat to Information Security and to disseminating information that will help mitigate these risks. Our newsletter is published periodically when there is news to report. We will not clutter your inbox with idle chatter when there is nothing significant or useful to say. This newsletter is available free of charge. Subscriptions are at the discretion of ManTech SRS Technologies.

Suggestions and comments are always welcome. If you do not wish to receive this newsletter, please e-mail us and we will gladly remove you from the list. All EDS-related correspondence should be sent to [Ronald.Hackett@ManTech.com](mailto:Ronald.Hackett@ManTech.com)

For information about [ManTech SRS Technologies' Document Detective electronic document review and sanitization toolkit](http://www.docdet.com/), please visit: <http://www.docdet.com/>

For a list of articles and information regarding EDS, including previous editions of this newsletter, please visit the Document Detective website and click on "The Threat."