Committee On Finance
Max Baucus, Ranking Member

NEWS RELEASE http://finance.senate.gov

For Immediate Release Contact: Carol Guthrie
Wednesday, July 26, 2006 (202) 224-4515

NEW REPORT FINDS LAX INTERNAL SECURITY AT IRS PUTS TAXPAYER FILES AT RISK FOR ILLEGAL REVIEW

IG has "little confidence" IRS is catching employees who may browse through tax files

Washington, DC – U.S. Senator Max Baucus (D-Mont.), Ranking Democrat on the Senate Finance Committee, commented today on reports that the IRS may be failing to ensure that taxpayers' records are not unlawfully accessed by employees of the agency. The Taxpayer Browsing Act of 1997 prohibits IRS employees from looking at individual taxpayer information and files without a specific professional purpose. A new report from the Treasury Inspector General for Tax Administration (TIGTA) says that most IRS business managers are not reviewing computer security reports to detect unauthorized access and security breaches within the agency. The security reports that managers should be reviewing show activity on the Integrated Data Retrieval System (IDRS), which contains taxpayers' names, birthdates, addresses, Social Security numbers, and other information.

"[W]e have little confidence that IRS managers are detecting potential unauthorized accesses of taxpayer information by employees," reads the report. **"Additionally, the IRS cannot ensure employees are complying with the security controls established to protect the IDRS."**

"With recent reports of security breaches at the VA and the Social Security Administration, it's unbelievable that IRS isn't doing what it takes to keep information safe in-house," said Baucus. **"What's on our taxes tells a lot about our lives, and that's why there are laws on the books to protect that information. If IRS isn't making sure privacy laws are followed even by its own employees, they're failing American taxpayers."**

The TIGTA review also revealed that the $2.4 million information technology system used to develop IDRS security reports did not meet IRS requirements when it was deployed in 2002. Upgrades to the system scheduled for deployment last year were not implemented, and the contract for the system improvements has now lapsed.

The Inspector General has recommended that the Chief of Mission Assurance and Security Services at IRS push managers to review the IDRS security reports, and make other change to managers' security-related requirements. The IG also recommended that a new contractor be hired on a priority basis to address the weaknesses of the current system to produce IDRS security reports.

The TIGTA report, "Increased Managerial Attention is Needed to Ensure Taxpayer Accounts are Monitored to Detect Unauthorized Employee Accesses" (Audit # 200520034) can be found at http://www.treas.gov/tigta/oa_auditreports_fy06.shtml.

# # #