January 14, 2003

The Honorable Duncan Hunter
Chairman
Committee on Armed Services
United States House of Representatives
2120 Rayburn House Office Building
Washington, DC 20515

The Honorable Ike Skelton
Committee on Armed Services
United States House of Representatives
2120 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Hunter and Representative Skelton:

We write to you as a nonpartisan coalition of organizations to urge Congress to stop further development of a Defense Advanced Research Projects Agency (DARPA) system called "Total Information Awareness" (TIA). TIA would put the details of Americans' daily lives under the scrutiny of government agents, opening the door to a massive domestic surveillance system. Congress should prohibit the development of TIA.

According to DARPA's own documents, TIA will collect and mine vast amounts of information on the American public, including telephone records, bank records, medical records, and educational and travel data. TIA would expand domestic intelligence activities to include the analysis of innocent people's personal information – credit card transactions, hotel reservations, or even prescription receipts. These so-called "non-traditional data sources" would put everyone's day-to-day transactions under government scrutiny.

The very workings of TIA would depend on access to massive amounts of personal information stored in electronic databases. By definition, the program is privacy-intrusive. As reported in the *Washington Times*, Administration officials have acknowledged that even the limited privacy protections for personal information provided under current law would have to be modified in order to fully implement the program.

Congress should not allow the Defense Department to develop unilaterally a surveillance tool that would invade the privacy of innocent people inside the United States. To date, the federal government has invested around $128 million in TIA and its component programs. The FY03 Defense appropriations bill included an additional $112 million. Yet, even as millions of dollars are spent to develop a hi-tech domestic surveillance system, the Defense Department's recent response to a Freedom of

Information Act request strongly suggests that privacy policy has received little consideration – if any - in TIA's development.

At a minimum, Congress should put the development of TIA on hold while it takes a closer look at the program through oversight hearings, investigations and reporting. These and other policy questions should be answered before any more federal money is spent on the program:

Why is the Department of Defense developing a domestic surveillance apparatus?

What databases of personal information would TIA envision having access to? What "non-traditional data sources" have already been used in testing and deployment of TIA?

How would current privacy law policies regulate TIA? What current laws would need to be amended to accommodate the source information needs of TIA?

What policy and technical research has been done on TIA and individual privacy?

What federal agencies would have interest in utilizing TIA and its component programs? For what purposes? What specific agencies have expressed interest in the program to date (according to press reports, the Information Awareness Office has already agreed to help the FBI and spoken to the Transportation Security Administration)?

What TIA applications have been delivered to federal agencies to date (according to press reports "Genoa," a TIA program, was sent to government agencies at the end of last year)? Has DARPA abandoned the "eDNA" program?

What private contractors, including private industry and academic researchers, have received funding for research and development of TIA? How much?

Have the TIA programs been evaluated or any determinations made as to effectiveness or feasibility? If so, what are the results of these evaluations or feasibility studies?

What information about innocent Americans would be swept up into government law enforcement and intelligence databases?

How would information culled from data-mining activities be used by law enforcement, intelligence, and other government agencies?

Would this system be effective? How would error rates and bureaucratic mistakes affect innocent individuals inside the United States? How can Congress ensure against misuse of this system for personal or political reasons?

Similar questions need to be asked about other initiatives that will vastly expand government collection and use of personal information, such as the CAPPS II (Computer Assisted Passenger Profiling System) program of the Transportation Security Administration.

We urge you to act immediately to stop the development of TIA and other similar programs that create massive public surveillance systems. At a time when Americans are calling for more privacy of personal information, this program would provide a backdoor to databases of private information. At a minimum, Congress should put such programs on hold and ask the tough policy questions up front, long before domestic surveillance systems scoop up Americans' personal information. Thank you for your consideration of this matter.

Sincerely,

American Civil Liberties Union
American Conservative Union
Americans for Tax Reform
Center for Democracy and Technology
Center for National Security Studies
Eagle Forum
Electronic Frontier Foundation
Electronic Privacy Information Center
Free Congress Foundation