

**COMMITTEE ON GOVERNMENT REFORM**  
**SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL**  
**RELATIONS AND THE CENSUS**  
**CONGRESSMAN ADAM PUTNAM, CHAIRMAN**



**OVERSIGHT HEARING**  
**STATEMENT BY ADAM PUTNAM, CHAIRMAN**

**Hearing topic: “*Can the Use of Factual Data Analysis Strengthen National Security? -Part One*”**

**Tuesday, May 6, 2003**  
**3:00 p.m.**  
**Room 2154 Rayburn House Office Building**

---

**OPENING STATEMENT**

---

In an effort to prevent future terrorist attacks and enhance law enforcement efforts, departments and agencies throughout the federal government have begun developing strategies that will assist in the identification of potential risks through the use of technology and information sharing. The truth is that there is a tremendous amount of information that already resides in the public venue. However, due to past practices of stovepipe mentalities and turf issues, much relevant information that could be of use or interest to law enforcement officials has not been easily accessible. In particular since September 11, 2001, it has been imminently clear that we must do a better job of compiling and sharing information that will provide enhanced opportunities for law enforcement and national security officials to identify potential risks...in advance. Federal agencies have utilized methodologies that facilitate database exploration for quite some time in an effort to root out waste, fraud and abuse. In fact, the recent highly public case of government credit card abuse was flushed out, and the perpetrators identified, through the use of “data mining” or “factual data analysis” as some would prefer it was called.

Now, a number of Federal agencies with responsibility for homeland security and law enforcement, are employing the lessons learned through the use of factual data analysis, or the conclusions drawn from this analytical process, to increase their ability to detect patterns and relationships within the masses of data they have access to in an effort to increase risk assessment capabilities. This hearing will examine whether the use of this process will successfully enhance efforts to strengthen law enforcement and national security. Does factual data analysis contribute to increased risk detection?

As we have previously established, factual data analysis is not a technology in and of itself. It is an analytical process that utilizes technology in an effort to identify patterns and relationships that were previously unknown. It has been used successfully in the private sector to craft specific marketing and sales programs. It

has been used successfully in the public sector to identify and address instances of waste, fraud, and abuse. The hope is that these same technological advances that aid marketers in identifying customers for their products and law enforcement in catching tax evaders or identifying welfare fraud, will also detect patterns that should raise suspicion among those working to improve our nation's security.

Today we have witnesses representing the Federal Bureau of Investigation (FBI), the Transportation Security Administration (TSA) and Defense Advanced Research Projects Agency (DARPA).

Each of these three agencies proposes to use factual data analysis or conclusions drawn from the process to enhance homeland security. Specifically we will be examining the FBI's Trilogy and related technology analysis tools, TSA's Computer Assisted Prescreening Process System (CAPPS II) and DARPA's Total Information Awareness (TIA). We have asked each of these witnesses to explain their agency's program and talk about the role factual data analysis is envisioned to play.

While each of these agencies proposals is different in its construct, and each may generate varying responses and levels of interest, the Subcommittee will seek to learn more about the source, accuracy, reliability, and security of the data that is accessed to determine risk assessment. Let me be clear...we are not here to compare one project to the other. We are not here to evaluate the strategic basis for these projects...we are here to examine the use of technology in the facilitation of this analytical process and the techniques, processes, and outcomes that are produced. We are here to listen and learn from these expert witnesses and to hear factual information about these projects. We also recognize that there is some concern and reluctance on the part of some of these witnesses to even be here today because of some of the press coverage about these projects. Today, we will examine the facts about how data will be compiled; what data will be assembled; what steps are taken to insure the accuracy and reliability of the data; how the data will be analyzed; and what will be done with the results, as well as how the privacy and personal freedom of the public will be protected by the process itself.

In two weeks, after gathering and evaluating the information that will be presented today, the Subcommittee will reconvene and examine this issue from a standpoint of privacy and personal freedom concerns in Part II of this hearing.

The Subcommittee believes this a good place to start from. From an oversight perspective, we look forward to working with these agencies as they continue to plan and implement their proposals for enhancing homeland security.