

December 12, 2003



# Information Technology Management

Terrorism Information Awareness  
Program  
(D-2004-033)

Department of Defense  
Office of the Inspector General

*Quality*

*Integrity*

*Accountability*

### **Additional Copies**

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at [www.dodig.osd.mil/audit/reports](http://www.dodig.osd.mil/audit/reports) or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

### **Suggestions for Future Audits**

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)  
Inspector General of the Department of Defense  
400 Army Navy Drive (Room 801)  
Arlington, VA 22202-4704

### **Defense Hotline**

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to [Hotline@dodig.osd.mil](mailto:Hotline@dodig.osd.mil); or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

### **Acronyms**

CAPPS II	Computer Assisted Passenger Prescreening System
DARPA	Defense Advanced Research Projects Agency
FAR	Federal Acquisition Regulation
IAO	Information Awareness Office
INSCOM	Army Intelligence and Security Command
TIA	Terrorism Information Awareness (formerly Total Information Awareness)
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

December 12, 2003

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION,  
TECHNOLOGY, AND LOGISTICS  
DIRECTOR, DEFENSE ADVANCED RESEARCH  
PROJECTS AGENCY

SUBJECT: Report on Terrorism Information Awareness Program (Report No.  
D-2004-033)

We are providing this report for your information and use. This audit was conducted to complete our response to congressional requests (See Appendix C). Section 8131 of the National Defense Appropriations Act for Fiscal Year 2004 (Public Law 108-87, September 30, 2003) eliminated funding for the majority of the Terrorism Information Awareness Program components. However, the content of this report remains applicable in the event that program concerns are resolved or DoD pursues similar technologies in the future.

We considered comments from the Director, Defense Research and Engineering and the Director, Defense Advanced Research Projects Agency on the draft of this report when preparing the final report. The comments were responsive in accordance with DoD Directive 7650.3; therefore, additional comments are not required.

We appreciate the courtesies extended to the staff. Questions should be directed to Colonel William Kelley at (703) 604-9312 (DSN 664-9312) or Ms. Pamela Varner at (703) 604-9265 (DSN 664-9265). See Appendix E for the report distribution. The team members are listed inside the back cover.

A handwritten signature in black ink, appearing to read "Thomas F. Gimble".

Thomas F. Gimble  
Acting Deputy Inspector General  
for Intelligence

## Office of the Inspector General of the Department of Defense

Report No. D-2004-033

December 12, 2003

(Project No. D2003CM-0056)

### Terrorism Information Awareness Program

#### Executive Summary

**Who Should Read This Report and Why?** DoD and Defense Advanced Research Projects Agency (DARPA) personnel involved in the development of the Terrorism Information Awareness (TIA) program or anyone interested in using sophisticated information technology that collects, stores, and analyzes information should read this report.

**Background.** This report completes our response addressing concerns of Senators Grassley, Nelson, and Hagel and discusses whether development of the DARPA TIA program included safeguards to ensure the technology was properly managed and controlled in an operational environment (See Appendix C). Section 8131 of the National Defense Appropriations Act for Fiscal Year 2004 (Public Law 108-87, September 30, 2003) eliminated funding for the majority of the TIA program components. However, the content of this report remains applicable in the event that program concerns are resolved or DoD pursues similar technologies in the future.

DARPA conducts research for DoD and was developing the TIA program to combat terrorist threats. The TIA research and development effort will integrate information technologies into a prototype system that will assist intelligence analysts in detecting, classifying, and identifying potential terrorist activities. The TIA research and development effort began in FY 2003. DARPA proposed in the President's FY 2004 Budget an estimated \$53.8 million in funding for development of TIA. That amount does not include however funding for the additional programs DARPA envisions as component programs of the TIA prototype. DARPA, in coordination with intelligence activities, is testing TIA capabilities in an operational research and development environment using real time feedback.

**Results.** A review of the TIA program to include the developmental contracts showed that although the TIA technology could prove valuable in combating terrorism, DARPA could have better addressed the sensitivity of the technology to minimize the possibility of any Governmental abuse of power and could have assisted in the successful transition of the technology into the operational environment. As a result, DoD risks spending funds to develop systems that may be neither deployable nor used to their fullest potential without costly revisions and retrofits. Because the audit was conducted in response to congressional requests, we did not perform a review of the DARPA management control program.

The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) in coordination with the Director, DARPA should perform a privacy impact assessment before TIA type technology research continues. In addition, USD (AT&L) should appoint a Privacy Ombudsman or equivalent official specifically for the development of Terrorism Information Awareness type technology who will ensure that

---

individual Terrorism Information Awareness type technology are scrutinized from a privacy perspective as a means of safeguarding individual privacy. The appointee, in consultation with the Office of the General Counsel, should conduct assessments on the impact of Terrorism Information Awareness type technology on privacy. (For detailed recommendations, see Recommendations, Management Comments and Audit Response.)

**Management Comments.** The Director, Defense Research and Engineering (DR&E), responding for the USD (AT&L), concurred with both recommendations. The Director, DR&E concurred with the importance of privacy impact assessments, stating that privacy impact assessments, focused on specific end-use applications, should precede all transitions to operational employment of TIA tools. The Director, DR&E stated that the decision to employ intelligence and synthetic data during the project development phase reflected deliberate consideration of privacy concerns at a level appropriate for a research effort. The Director, DR&E also stated that the report should have concluded that the TIA project did not violate privacy policies of the United States. In addition, the Director, DR&E stated that in the absence of guidance on privacy impact assessments, DARPA restricted developmental efforts to intelligence and synthetic databases, formed review boards, and implemented DARPA research into privacy safeguards.

The Director, DARPA stated that our report did not address the concerns raised by several U.S. Senators (Senators Grassley, Hagel, and Nelson) that DARPA was developing a system for domestic law enforcement for which it had no statutory duty to do so. The Director, DARPA stated that although DARPA acknowledged that TIA could be used by law enforcement, the report should have explicitly stated that DARPA was not developing a system for domestic law enforcement. The Director, DARPA stated that any use by law enforcement would have to be approved by Congress as well as other authorities. The Director, DARPA also stated that the report should have been clearer that a privacy impact assessment was not required. See the Management Comments section of the report for a complete text of the comments.

**Audit Response.** Although the report stresses that DoD and DARPA need to be proactive and address policy and privacy measures at the earliest stages, the report does not assert or conclude that any privacy violations have occurred. In response to the concerns of the Director, DARPA that the report does not address congressional concerns, we have included in Appendix C our responses to Senators Grassley, Hagel, and Nelson, which clearly set forth our objectives for this audit. Relating to the intended end uses of TIA, senior USD (AT&L) officials in briefings had clearly indicated that TIA had potential usage by both the intelligence and law enforcement communities. In response to the Director, DARPA comments on the privacy impact statement, the report clearly sets forth our position that, in the case of TIA, prudence would dictate that a requirement for a privacy impact assessment be done as a best business practice though no firm requirement exists.

# Table of Contents

---

<b>Executive Summary</b>	i
<b>Background</b>	1
<b>Objectives</b>	3
<b>Finding</b>	4
Privacy Protection	
<b>Appendixes</b>	
A. Scope and Methodology	16
B. Congressional Requests	17
C. Department of Department, Office of the Inspector General Congressional Responses	21
D. Terrorism Information Awareness Subsystems	28
E. Report Distribution	30
<b>Management Comments</b>	
Director, Defense Research, and Engineering	32
Defense Advanced Research Projects Agency	34

---

## Background

This audit was initiated to complete our response to concerns Senators Grassley, Hagel, and Nelson raised in letters to the OIG DoD. The report discusses whether the development of the Defense Advanced Research Projects Agency (DARPA) Terrorism Information Awareness (TIA) program included safeguards to ensure the technology was properly managed and controlled in an operational environment. To ease public concerns, DARPA changed the name of the program in May 2003 from the Total Information Awareness program.

**Defense Advanced Research Projects Agency.** DARPA is an agency of DoD under the direction, authority, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) and the Director of the Defense Research and Engineering. DARPA conducts research and development for DoD. DARPA is charged with maintaining the technological superiority of the U.S. military and preventing a technological surprise that would harm our national security. The Director of DARPA oversees eight offices. The Information Awareness Office (IAO) is one of those offices.

**Information Awareness Office.** In response to the attack of September 11, 2001, DARPA established the IAO in January 2002. The IAO was designed to integrate several existing information technology programs for which DARPA was responsible. Those programs focused on using information technology to combat terrorism.

**Terrorism Information Awareness Program.** The TIA program is a research and development effort that began in FY 2003. The program was designed to increase the probability that authorized agencies within the United States could preempt terrorist actions. The TIA program attempts to integrate information technologies into a prototype that could determine the feasibility of searching vast quantities of data as well as determines links or patterns in the data that are indicative of terrorist activities.

The TIA program seeks to develop information technology in three areas. Those areas are language translation, data search with pattern recognition and privacy protection, and advanced collaborative and decision support tools. Language translation technology would enable the rapid analysis of foreign languages, both spoken and written, and allow analysts to quickly search the translated materials for clues about emerging threats. The data search, pattern recognition, and privacy protection technologies would permit analysts to search vast quantities of data for patterns that suggest terrorist activity while at the same time controlling access to the data, enforcing laws and policies, and ensuring detection of misuse of the information obtained. The collaborative reasoning and decision support technologies would allow analysts from different agencies to share data.

Although DARPA was developing the technology, it did not intend to use the TIA prototype system. DARPA would have instead turned over the prototype for adoption to DoD and other Federal agencies.

---

In its May 2003 report to Congress, DARPA identifies 15<sup>1</sup> component programs that will potentially contribute to the overall TIA model. The report also included a proposed FY 2004 President's budget submission for TIA of \$53.8 million. The estimate, however, is only for the TIA development effort and does not include any of the other programs that will potentially be included in the TIA network. See Appendix D for a brief explanation of the subsystems as well as a breakdown of the budget for each.

Section 8131 of the National Defense Appropriations Act for Fiscal Year 2004 (Public Law 108-87, September 30, 2003) eliminated funding for the majority of the TIA program components. The language in the Act directed DARPA to terminate the IAO but permitted continuation of four research projects for foreign intelligence. Of the four components Congress funded, three were initially included in the TIA program.

**DoD Partners in TIA Experiments.** For testing TIA capabilities, DARPA and the U.S. Army Intelligence and Security Command (INSCOM) created an operational research and development environment that uses real time feedback. The main node of TIA is located at INSCOM with additional TIA nodes located at subordinate INSCOM commands and at other participating organizations throughout DoD and the intelligence community. INSCOM is testing TIA technologies using information gathered by routine intelligence means.

The National Security Agency, the Defense Intelligence Agency, the Central Intelligence Agency, the DoD Counterintelligence Field Activity, the U.S. Strategic Command, the Special Operations Command, the Joint Forces Command, and the Joint Warfare Analysis Center are either participating or plan to participate with DARPA and INSCOM to test TIA capabilities.

**Other Federal Agency Participation in TIA Experiments.** In addition to its DoD counterparts, DARPA has discussed with the Federal Bureau of Investigation and other non-DoD Federal agencies in support of law enforcement and counter terrorism efforts possible participation in the TIA technology experiments. DARPA has not yet established any formal agreement outside of DoD.

---

<sup>1</sup>DARPA originally had 16 potential component programs, but FutureMap was subsequently discontinued after congressional and public scrutiny.



---

## **Objectives**

Our overall audit objective was to assess whether DARPA included the proper controls in the developmental contracts for the TIA program that would ensure that the technology, when placed in an operational environment, is properly managed and controlled.

We did not perform a review of the management control program because the audit was conducted in response to congressional requests (See Appendix B).

---

## Privacy Protection

Although the DARPA development of TIA-type technologies could prove valuable in combating terrorism, DARPA could have better addressed the sensitivity of the technology to minimize the possibility for Governmental abuse of power and to help ensure the successful transition of the technology into an operational environment. Several factors contributed to the condition.

- DARPA did not implement the best business practice of performing a privacy impact assessment.
- USD (AT&L) initially provided limited oversight of the TIA development and did not ensure that DARPA included in the effort the appropriate DoD policy, privacy, and legal experts.
- DARPA efforts historically focused on development of new technology rather than on the policies, procedures, and legal implications associated with the operational use of technology.
- The DARPA position was that planning for privacy in the operational environment was not its responsibility because TIA research and experiments used synthetic artificial data or information obtained through normal intelligence channels.

As a result, DoD risks spending funds to develop systems that may not be either deployable or used to their fullest potential without costly revision.

## Potential of TIA to Combat Terrorism

Since September 11, 2001, the Federal Government has emphasized improving communication and information sharing among intelligence, counterintelligence, and law enforcement communities to prevent terrorist attacks. The congressional joint inquiry concluded that technology is not being effectively employed. Even though technology development is one of the Nation's greatest advantages, problems persist among the intelligence community in the area of collaboration.

To resolve collaboration problems, DoD and Congress believe that TIA--once developed and proven effective--could help Federal agencies work together as well as improve their ability to detect and counter future terrorist attacks. Based on public concern that the TIA program will enhance the Government's power along with the fear of potential abuse and misuse of the system, the TIA program has generated substantial controversy and criticism.

**Congressional Concerns.** In June 2002, DoD announced that DARPA would develop the TIA program. Since that time, Congress has repeatedly expressed concern about the technology the program would use and associated privacy implications. In February 2003, for example, Congress enacted Public Law 108-7 that stopped all funding for the proposed TIA program until DARPA and the

---

Pentagon could prove that the program does not violate privacy rights. Specifically, the amendment limited DoD ability to implement TIA without prior congressional approval and required a report within 90 days. The report, which DARPA completed on May 20, 2003, addresses concerns for privacy and includes program milestones and budget information for the TIA program.

Still voicing concerns, Congress eliminated funding for the majority of the TIA components in Section 8131 of the National Defense Appropriations Act for Fiscal Year 2004 (Public Law 108-87, September 30, 2003). The language in the Act directs that DARPA terminate the IAO but permits continuation of four research projects for foreign intelligence. Of the four components Congress funded, three were initially included in the TIA program.

**Congressional Concerns About Privacy Not New.** Congress has criticized the Transportation Security Agency's Computer Assisted Passenger Prescreening System II (CAPPS II) because the system potentially impacts the public's right to privacy and civil liberties. CAPPS II is a computer system that can screen the backgrounds of airline passengers looking for potential ties to terrorism by searching Government and commercial databases in an effort to make determinations about individuals as potential aviation security risks. The Transportation Security Agency responded to the concerns by narrowing the scope of how CAPPS II uses passenger information and limited the length of time the information would be collected and maintained. Congress stopped all CAPPS II funding until completion of a General Accounting Office review.

## **Sensitivity of TIA Technology and Best Business Practice**

DARPA could have better addressed the sensitivity of the TIA technology and implemented the best business practice of performing a privacy impact assessment that would have helped ensure successful transition of the technology to an operational environment. DoD and DARPA have indicated two potential uses for the TIA technology, one of which would gather foreign intelligence about non-Americans and the other domestic information for intelligence and law enforcement use. For domestic law enforcement purposes, DARPA should consider more fully during development the impact of the technology on an individual's privacy by conducting a privacy impact assessment. Statute does not require a privacy impact assessment for systems that involve intelligence activities. However, an assessment could provide decisionmakers with enough information to help them make fully informed policy, program, system design, funding, and procurement decisions that are based on an understanding of the privacy implications, the involved risks, and the options available for avoiding or mitigating risks. A privacy impact assessment could also help reduce the risk of terminating or modifying TIA type technology after implementation to comply with privacy laws and regulations.

**Electronic Government Act of 2002.** Public Law 107-347, the Electronic Government Act of 2002, requires that Federal agencies complete a privacy impact assessment before developing or procuring information technology systems, or initiating new collections of information. A privacy impact

---

assessment is an explanation of how an agency will build privacy protections into new information systems. Program personnel complete questions on data requirements and protection before the system is developed. The agency Chief Information Officer or equivalent reviews the completed privacy impact assessments before making the assessment public through either the agency's Web site, publication in the Federal Register, or other sources.

The Office of Management and Budget is responsible for issuing guidance specifying the required contents of a privacy impact assessment. The guidance has not been disseminated. Once published and disseminated, Government agencies will be required to conduct the statutorily mandated privacy impact assessment.

**Privacy Impact Assessment as a Best Business Practice.** A privacy impact assessment is a best business practice that certified information system auditors in the public, private, and Federal sectors use. In the President's FY 2001 budget, the President announced an initiative that would make privacy impact assessments a regular part of development for new Government computer systems. The privacy impact assessment is a prudent practice from the standpoint that the assessment provides a framework that ensures privacy is considered throughout the business or project development cycle particularly at the conceptual and requirements analysis stage as well as at the final design approval and funding stage. A privacy impact assessment is typically a public document that explains how an agency will take privacy considerations into account when purchasing and creating new information systems as well as when initiating collections of information.

The requirement to perform a privacy impact assessment does not apply to systems that involve intelligence activities and because DARPA was using intelligence and synthetic data in the development and testing activities of TIA, a privacy impact assessment was not required. Because DARPA anticipated that TIA would be used for domestic law enforcement, a privacy impact assessment should have been performed. In addition, DARPA should have performed a privacy impact assessment because the development of TIA occurred simultaneously with the transition of the TIA technology in to the operational environment. Because of the nature of the transition, DARPA should ensure that privacy is considered at the beginning of the development cycle and should implement controls that protect privacy during development. Those controls should ensure the technology is usable from a legal standpoint in the operational environment for both the intelligence community and the law enforcement community. In performing a privacy impact assessment, DARPA should gain the information that they need to work privacy requirements and constraints of the end users into the project development cycle. DARPA has acknowledged that privacy and civil liberty issues would have to be carefully considered and resolved in advance of deployment; however, DARPA may be able to avoid costly retrofits by implementing privacy controls during the development process as opposed to after.

**Internal Revenue Service's Privacy Impact Assessment Best Practice.** The Federal Chief Information Officer's Council endorsed the Internal Revenue Service's privacy impact assessment as a Chief Information Officers Council best

---

practice for evaluating privacy risks on information systems. At the Internal Revenue Service, privacy issues must be addressed when systems are being developed. The privacy impact assessment process ensures compliance with applicable laws and regulations. The privacy impact assessment incorporates an analysis of privacy into the development life cycle of the system so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design. The privacy impact assessment process consists of privacy training, gathering data on privacy issues, identifying and resolving the privacy risks, and approval by the Internal Revenue Service privacy advocate. Both the system owner and system developers must work together to complete the privacy impact assessment. The data must be relevant and necessary and accomplish the purpose of the system. The data must also be complete, accurate, and timely. Precise rules must be established not only for the length of time information is kept but for assuring that the information is properly eliminated at the end of that time.

**TIA Use by Domestic Law Enforcement.** DARPA, USD (AT&L), and other senior DoD leaders envisioned that TIA would be used by both DoD and foreign intelligence communities as well as law enforcement. The use of TIA by law enforcement is what has caused the greatest public concern over privacy. The USD (AT&L) briefed the press that “if TIA proves useful, it would be then turned over to the intelligence, counterintelligence and law enforcement communities as a tool to help them in their battle against domestic terrorism.” During confirmation hearings, the Assistant Secretary of Defense for Homeland Defense stated, “it is my understanding that if that technology were to be developed, that the implementation, the operational use of that technology in a domestic context would be external to the Department of Defense, that it would migrate from DARPA out into the civilian law enforcement community.” The Assistant Secretary reconfirmed that position by stating that it was not the intent of the DoD to operate TIA. “Once the technology is developed utilizing the resources of the Department of Defense, the intent has been to transfer that technology out to the civilian community, particularly to civilian law enforcement agencies for their employment in order to, in this instance, locate that weapon of mass destruction.” Figure 1 depicts both foreign intelligence use of TIA and law enforcement use of TIA. DARPA experiments are being accomplished in the foreign intelligence and counterintelligence community; however, DARPA needs to consider how TIA will be used in terms of law enforcement to ensure that privacy is built into the developmental process.

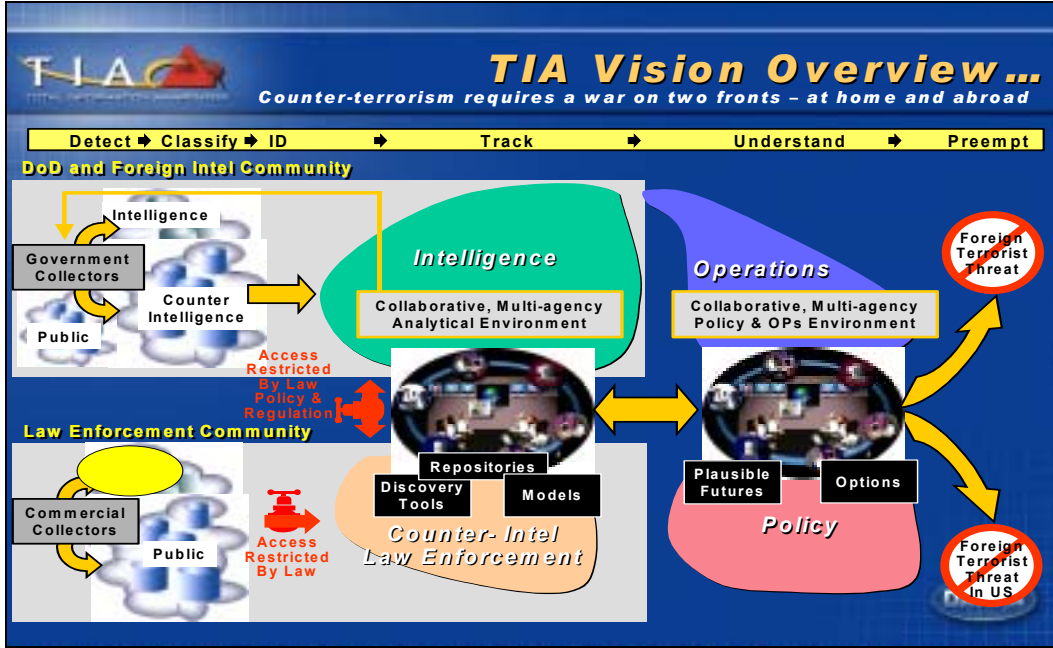


Figure 1. TIA Use by Law Enforcement Community

## TIA Approval and Oversight

**TIA Program Approval.** USD(AT&L) announced in November 2002 that DARPA had established the TIA program to aid in the antiterrorist efforts of DoD. According to the Director, DARPA established TIA to leverage the existing counter terrorism technologies with those new research projects being developed after the September 11, 2001, attack. DARPA briefed the TIA program to USD (AT&L), at which time USD (AT&L) approved the program and deemed it worthy of pursuit.

**TIA Program Oversight.** USD (AT&L) initially provided limited oversight of TIA development and approved the development without requiring that DARPA obtain support from DoD experts in policy, privacy, and legal matters to help ensure successful transition of the technology into an operational environment. It was not until Congress and the public began to question the developmental effort and its impact on privacy that USD (AT&L) and DARPA took action to specifically address privacy concerns. In response to concerns, USD (AT&L) established two boards that would provide oversight of the TIA program. DARPA responded to the issue of privacy by developing certain technical safeguards.

**TIA Oversight Boards.** DoD established two boards, one an internal oversight board and the other an outside advisory committee board, that would work with DARPA during the development of TIA. The boards help ensure that TIA is developed and operationally transitioned consistent with privacy laws.

---

**Internal Oversight Board.** The internal TIA oversight board is composed of various DARPA and DoD officials and chaired by the USD (AT&L). The primary function of the board is to establish policies and procedures for TIA as well as related technologies and establish protocols for transferring those technologies to entities outside the DoD. The internal oversight board had its initial meeting in February 2003.

**Outside Advisory Committee Board.** The Technology and Privacy Advisory Committee is an external Federal advisory committee. The committee advises the Secretary of Defense on policy and legal issues raised during development or with regard to any potential application of TIA technologies. The primary duty of the committee is to prepare a written report for the Secretary of Defense about the use of the advanced information technology to identify potential terrorist activity. The committee holds meetings as required and has held five meetings in the past year.

**Technical Safeguards.** In its development of TIA, DARPA sponsored research of privacy safeguards and options that would balance security and privacy issues. Those measures, however, were not as comprehensive as a privacy impact assessment would have been in scrutinizing TIA technology.

**Genisys Privacy Protection.** The Genisys Privacy Protection contractor is working to develop techniques to allow authorized analysts to search a collection of databases while providing a realistic degree of privacy protection for U.S. citizens who may be represented in those databases. The program will develop access control mechanisms to restrict the release of sensitive data only to authorized users. The contractor is also working to develop inference control, access control, and analyst tracking techniques to restrict access to private information and monitor usage of private information.

**Center for Strategic and International Studies.** The Center for Strategic and International Studies is developing approaches for protecting private information accessed by the Government. The Center for Strategic and International Studies will try to determine whether new models of oversight exist and structural or legal privacy protections are available, that would permit some use of pattern-based queries. The Center is also reviewing other promising technologies that aid in the fight against terrorism but protect against Government abuse and unacceptable intrusions on privacy.

**The Arlington Institute.** DARPA contracted with the Arlington Institute for advice on the public's privacy issues. The Institute is working to understand Government concerns and safeguards relative to privacy issues, to clearly understand the legitimate concerns of the Government for gathering information about potential terrorism, and to provide ongoing advice about communication. The ultimate goal of the Arlington Institute is to help design aspects of IAO programs.

**The Potomac Institute for Policy Studies.** DARPA contracted with the Potomac Institute for Policy Studies to review the availability of

---

useful informational databases, electronic transactional data, and the propriety of access to such information in the context of protecting Americans from terrorists and terrorism.

**Information, Security, and Technology 2002 Study.** DARPA commissioned a study that would examine specific technological problems for safeguarding privacy. The study, which was not policy oriented, concluded that technologies exist that permit surveillance while minimizing exposure of individual information. Those technologies included an automated record of individuals accessing the database information, the ability to hide an individual's identity while conducting searches of databases with millions of records, and the ability to segregate databases and to block access to people without authorization. The study was not a critique or endorsement of any specific DARPA program and did not attempt to make policy recommendations.

## **Technology Developers not Users**

**DARPA Develops Technology.** In 1958, the Secretary of Defense established DARPA as the only DoD research agency without a specific operational mission. Its charter was radical innovation. DARPA is comprised primarily of engineers who do not typically create policy. Because the DARPA mission has in the past focused on development of new technology and because they are not the users of the technology, DARPA did not fully consider the sensitivity of the technology nor did they include DoD experts in privacy, policy, and legal issues for TIA development efforts.

**Involvement of Experts in Policy, Privacy, and Legal Issues for TIA Experiments.** Without a requirement to obtain support from DoD experts on policy, privacy, and legal issues, DARPA could have better addressed privacy concerns in its development of TIA to help ensure successful transition of the technology into an operational environment. Specifically, DARPA did not include in TIA experiments DoD representatives from the privacy, policy, and legal communities. DARPA stated in the May 2003 report to Congress that the goal of TIA research and development is to have the intelligence, counterintelligence, operational, and policy domains working together comprehensively to counter terrorist attacks. Figure 2 from DARPA briefing charts reiterates a lack of participation in TIA experiments by policy makers within DoD.





Figure 2. Participation in TIA Experimental Process

## Legally Obtained and Synthetic Data

**Use of Information.** DARPA did not anticipate privacy issues in an operational environment, in part, because the research and testing of TIA depended strictly on the use of information that was either obtainable through normal DoD intelligence channels or artificial synthetic data that was specifically generated to resemble real world transactions. DARPA stated that the use of obtainable intelligence and synthetic artificial data does not implicate the privacy interests of U.S. persons. However, included in the TIA technology are data search and analysis tools, which depend on different types of data contained in databases. The TIA use of information from different sources does raise the risk to personal privacy when that information is aggregated and made accessible to intelligence, law enforcement, and other security personnel for purposes other than the original intent.

**Legally Obtained Information.** DARPA affirms that organizations from DoD intelligence communities participating in TIA development provided the foreign intelligence and counter-intelligence information for TIA experiments. The information was obtained and usable by the Federal Government under existing laws, regulations, and policies.

**Synthetic Data.** Because the TIA experiments are using synthetic data, which is artificial data generated for research, no U.S. citizen privacy implications were associated with its use. The synthetic data resembles and models real-world patterns of behavior.

---

**Privacy Act of 1974.** Public Law 93-579, Privacy Act of 1974, provides that the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies. The increasing use of computers and sophisticated information technology has increased the threat to individual privacy that can occur when collecting, maintaining, using, and disseminating personal information. The Privacy Act provides certain safeguards against the invasion of privacy for an individual. One of the purposes of the Privacy Act is to permit individuals to determine which records pertaining to them are collected, maintained, or disseminated to other agencies and grants individuals the right to access and amend those records if they are not accurate, relevant, current, or complete. DoD policy prohibits the disclosure of personally identifiable records that Government agencies maintain without a person's consent.

**Federal Acquisition Regulation.** The Federal Acquisition Regulation (FAR) Part 52, "Protection of Privacy and Freedom of Information," prescribes to Government contracts policies and procedures that apply to the requirements of the Privacy Act of 1974. The FAR requires that contracting officers insert Privacy Act clauses 52.224-1 and 52.224-2 in contracts. When the design, development, or operation of a system of records on individuals is required to accomplish an agency function, the clauses require that contractors comply with the Privacy act of 1974.

**System Procurement.** Focused on research and testing, DARPA awarded three contracts and one Other Transaction Agreement for developing TIA architecture. The three contracts and the other transaction agreement provided for development of the following technologies and programs: the Assured Transition and Transformation Prototype Systems Technologies; the Adaptive Red Teaming and Experimentation Program; the Closed-Loop, End-To-End Prototype System For Early Warning and Decision Making; and the Component Technology Interface for TIA. The other transaction agreement includes one subcontractor deliverable for technology integration support for "Privacy Protection for Integrated Intelligence Operations." The three contracts did not include any deliverables that addressed privacy issues associated with the development of the TIA architecture. Because they are using legally obtained information or synthetic data, DARPA officials stated that including the FAR clause for privacy in either their solicitations for TIA or in the TIA contracts was not necessary. Furthermore, the FAR does not apply to other transaction agreements.

## Conclusion

DoD and DARPA could have better addressed the sensitivity of the TIA technology and planned for its transition into an operational environment more effectively. Because of the lack of foresight, DoD risks spending funds to develop systems that may not be deployable or may not be used to their fullest potential without costly revisions or retrofits. Moreover, the potential use of this technology by domestic law enforcement and the DARPA lack of consideration for the sensitivity of the TIA type technology has raised the effort to an unnecessarily heightened level of awareness and concern for both Congress and

---

the public. Both DoD and DARPA need to address policy, privacy, legal, and protective measures at the earliest stages of the development to ensure that requirements are analyzed and appropriate decisions are made about the data and system design. To provide proper safeguards in technology design, development, and testing, DARPA needs to address any impacting privacy concerns for each application of TIA type technology. For example, experts in policy, privacy, and legal issues, if included in the experiments, could assist DARPA developers and analysts in addressing the types of data available for use, how to appropriately and legally use the data obtained, and address whether the operation of the system presents any threats to the privacy and civil liberties of U.S. citizens.

## **Management Comments on the Overall Report and Audit Response**

Comments on the overall report were received from the Director, Defense Research, and Engineering and the Director, DARPA. Full management comments can be found in the Management Comments section.

**Director, Defense Research and Engineering Comments.** The Director, Defense Research and Engineering (DR&E) responded for USD (AT&L). The Director, DR&E concurred with the importance of privacy impact assessments, stating that privacy impact assessments, focused on specific end-use applications, should precede all transitions to operational employment of TIA tools. The Director, DR&E stated that the decision to employ intelligence and synthetic data during the project development phase reflected deliberate consideration of privacy concerns at a level appropriate for a research effort. The Director, DR&E also stated that the report should have concluded that the TIA project did not violate privacy policies of the United States. According to the Director, DR&E, the report serves a useful purpose in discussing privacy concerns and protective processes that should be addressed during transition of research projects to domestic applications. In the absence of guidance from the Office of Management and Budget on the contents of a privacy impact statement, the Director, DR&E stated that DARPA restricted developmental efforts to intelligence and synthetic databases, formed review boards, and implemented DARPA research into privacy safeguards.

**Director, Defense Advanced Research Projects Agency.** The Director, DARPA stated that the report did not address the concerns raised by several U.S. Senators (Senators Grassley, Hagel, and Nelson) that DARPA was developing a system for domestic law enforcement for which it had no statutory duty to do so. The Director, DARPA stated that the report should have explicitly stated that DARPA was not developing a system for domestic law enforcement. The Director, DARPA stated that DARPA acknowledged in its February 2003 Strategic Plan and the May 2003 report required by the Wyden Amendment that TIA could be used by Law Enforcement; however, any use by domestic law enforcement would have to be approved by Congress as well as other authorities. The Director, DARPA stated that the report should have been clearer that a privacy impact assessment was not required. In addition, the Director, DARPA

---

acknowledged that if a law enforcement organization wanted to use TIA products, it would be required to perform a privacy impact assessment.

**Audit Response.** Although the report stresses that DoD and DARPA need to be proactive and address policy and privacy measures at the earliest stages, the report does not assert or conclude that any privacy policy violations have occurred. In response to the concerns of the Director, DARPA that the report does not address congressional concerns, we have included in Appendix C our responses to Senators Grassley, Hagel, and Nelson, which clearly set forth our objectives for this audit. Relating to the intended end uses of TIA, senior USD (AT&L) officials in briefings clearly indicated that TIA had potential usage by both the intelligence and law enforcement communities. As the report states, USD (AT&L) briefed the press that if TIA proved useful, it would be turned over to the intelligence, counterintelligence, and law enforcement communities as a tool in the battle against domestic terrorism. In confirmation hearings, the Assistant Secretary of Defense for Homeland Defense stated that it was his understanding that if TIA technology were developed, the operational use of that technology in a domestic context would migrate into the civilian law enforcement community. In response to the Director, DARPA comments on the privacy impact statement, the report clearly sets forth our position that, in the case of DARPA, although no firm requirement existed for a privacy impact statement, prudence would dictate that one be done as a best business practice—refer to the report section on page 6 entitled *Privacy Impact Assessment as a Best Business Practice*.

## **Recommendations, Management Comments and Audit Response**

We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics USD (AT&L) in coordination with the Director, Defense Advanced Research Projects Agency:

**1. Perform a Privacy Impact Assessment before Terrorism Information Awareness type technology research continues. Specifically, the privacy impact assessment at a minimum should:**

- a. Identify any personally identifiable information associated with business processes.**
- b. Document any collection, use, disclosure, and destruction of personally identifiable information.**
- c. Assess potential privacy risk and the options available for mitigating that risk.**
- d. Ensure that accountability for privacy issues is clearly incorporated in the program.**
- e. Create a consistent format and structured process for analyzing both technical and legal compliance with relevant regulations.**

---

**Director, DR&E Comments.** The Director, DR&E concurred with comment, stating that the establishment of additional oversight mechanisms by USD (AT&L) through the Internal Oversight Board and the Outside Advisory Committee Board (Technology and Privacy Advisory Committee) are equivalent processes to privacy act assessments. The Director, DR&E stated that ongoing reviews of TIA projects provide effective assessments of data employment and knowledge products during the research and technology development phase. The Director, DR&E also stated that formal privacy impact assessments should be conducted, reviewed, and approved before authorizing use of TIA tools in operational applications.

**Audit Response.** The Director, DR&E comments satisfy the intent of the recommendation.

**2. Appoint a Privacy Ombudsman or equivalent official specifically for the development of Terrorism Information Awareness type technology who will ensure that individual Terrorism Information Awareness type technology are scrutinized from a privacy perspective as a means of safeguarding individual privacy. The official, in consultation with the Office of the General Counsel, should:**

**a. Conduct assessments on the impact of Terrorism Information Awareness type technology on privacy.**

**b. Ensure that the Terrorism Information Awareness type technologies strike the proper balance between the need for identifying information and the individuals' right to be protected against unwarranted intrusions into his or her personal privacy.**

**c. Ensure that the collection, use, and disclosure of identifying information is authorized by existing law, to include the Privacy Act.**

**d. Ensure that appropriate safeguards are adopted that will protect the confidentiality of the information during the development of the technology and when transitioned to another DoD or Federal agency.**

**Director, DR&E Comments.** The Director, DR&E concurred with the recommendation.

---

## Appendix A. Scope and Methodology

We performed this audit from January 2003 through October 2003 in accordance with generally accepted government auditing standards. We visited DARPA headquarters in Arlington, Virginia, and interviewed DARPA personnel from the IAO and the Contract Management office. We also interviewed officials from the Defense Privacy Office; the Office of the Assistant Secretary of Defense for Homeland Defense; the Office of the Assistant to the Secretary of Defense for Intelligence Oversight; the Office of General Counsel; and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. During the interviews, we obtained pertinent reports and knowledge on the Terrorism Information Awareness Program.

During the audit, we reviewed the Federal laws and DoD directives and regulations that relate to the protection of privacy. We reviewed the DARPA solicitation for development of TIA as well as three developmental contracts, one other transaction agreement, and contractual supporting documentation to include the four statements of work. In addition, we reviewed four statements of work for technical safeguard contracts funded by DARPA and analyzed the DARPA commissioned Information, Security, and Technology 2002 Study. The scope of the audit was limited in that we did not perform a review of the management control program because the audit was conducted in response to congressional requests.

**Use of Computer-Processed Data.** We did not use computer-processed data to perform this audit.

**General Accounting Office High-Risk Area.** The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the DoD high-risk area identified as “Effectively manage information technology investments.”

### Prior Coverage

No prior coverage has been conducted on TIA during the last 5 years.

## Appendix B. Congressional Requests

MAX BAUCUS, MONTANA, CHAIRMAN  
JOHN D. ROCKEFELLER IV, WEST VIRGINIA  
TOM DASCHLE, SOUTH DAKOTA  
JOHN SREALUX, LOUISIANA  
KENT CONRAD, NORTH DAKOTA  
BOB GRAHAM, FLORIDA  
JAMES M. ZEPPORDS II, VERMONT  
JEFF BINGAMAN, NEW MEXICO  
JOHN F. KERRY, MASSACHUSETTS  
ROBERT G. TORRES, NEW JERSEY  
BLANCHE L. LINCOLN, ARKANSAS

JOHN ANSELL, STAFF DIRECTOR  
KOLAN DAVIS, REPUBLICAN STAFF DIRECTOR AND CHIEF COUNSEL

### United States Senate

COMMITTEE ON FINANCE

WASHINGTON, DC 20510-6200

November 22, 2002

The Honorable Joseph E. Schmitz  
Inspector General  
Department of Defense  
The Pentagon  
Washington, D.C.

Dear Inspector General Schmitz:

The Department of Defense (DoD) recently provided information regarding a research program entitled "Total Information Awareness" (TIA). Unfortunately, DoD's comments only provide few answers and invite many more questions.

TIA is a research program that would review a vast amount of information including credit card purchases, driver's license and car rentals for the benefit of law enforcement officials. In addition, news reports state that neither the Department of Justice or the Federal Bureau of Investigations has been consulted on TIA.

I am at a loss to understand why DoD resources are being spent on research for domestic law enforcement. In addition, to develop such a program in a vacuum from federal law enforcement seems to be asking for taxpayer dollars to be sent down the drain.

As I assume the responsibility of Chairman of the Finance Committee, which has oversight of certain financial reporting, I would ask that your office conduct a complete and thorough review of the TIA program.

This review should include:

- 1) What is the statutory authorization for TIA?
- 2) What are the parameters and scope of TIA?
- 3) How was TIA selected to be funded?
- 4) How was Admiral Poindexter selected to head TIA?

- In addition, please review the awarding of the consultant contract for Admiral Poindexter.
- 5) What coordination has the program had with federal law enforcement officials?

This should include details of what input was received prior to funding.

- 6) What protections are in place to ensure civil liberties are not violated?

---

I ask that you meet with Mr. Dean Zerbe, Chief Investigative Counsel, of the Senate Finance Committee to discuss further this important matter at (202) 224-5315. Thank you for your time and courtesy.

Cordially yours,

A handwritten signature in black ink that reads "Chuck Grassley". The signature is written in a cursive, slightly slanted style.

Charles E. Grassley  
Ranking Member



CHUCK HAGEL  
NEBRASKA  
248 RUSSELL SENATE OFFICE BUILDING  
(302) 224-4234  
(888) 224-6060 TTY/TDD

United States Senate  
WASHINGTON, DC 20510-2706

FOREIGN RELATIONS  
BANKING, HOUSING, AND URBAN AFFAIRS  
ENERGY AND NATURAL RESOURCES  
BUDGET  
SPECIAL COMMITTEE ON AGING

December 2, 2002

The Honorable Joseph E. Schmitz  
Inspector General  
Department of Defense  
The Pentagon  
Washington, DC

Dear Inspector General Schmitz:

I am writing to express my concern regarding the Total Information Awareness (TIA) Program, conducted through the Defense Advanced Research Projects Agency at the Department of Defense.

Since 1878, the law of the United States has been to separate the military from domestic police functions and law enforcement. The Posse Comitatus Act, and this separation of responsibilities, has helped foster strong public support and respect for our men and women in uniform. In the Homeland Security legislation signed by President Bush on November 25, Section 886 specifically confirmed the importance of the Posse Comitatus Act. Therefore, I am concerned to hear of a \$10 million program at the Department of Defense to conduct research for domestic law enforcement technology.

My colleague, Senator Grassley, wrote to you on November 22 requesting a complete and thorough review of the TIA program. I strongly support the efforts of Senator Grassley on this matter, and would like a copy of any report you may issue in response to his questions.

Thank you for your consideration of this request, and I look forward to your reply.

Sincerely,



4003 6TH AVENUE  
SUITE 9  
Kearney, NE 68845  
(308) 236-7602

294 FEDERAL BUILDING  
100 CENTENNIAL MALL NORTH  
LINCOLN, NE 68508  
(402) 478-1400

11301 DAVENPORT STREET  
SUITE 2  
OMAHA, NE 68154  
(402) 758-8981

115 RAILWAY STREET  
SUITE C102  
SCOTTSBUFF, NE 68361  
(308) 632-6032

chuck\_hagel@hagel.senate.gov



**United States Senate**  
WASHINGTON, DC 20510-0005

BILL NELSON  
FLORIDA

December 13, 2002

The Honorable Joseph E. Schmitz  
Inspector General  
Department of Defense  
400 Army Navy Drive  
Arlington, VA 22202

Dear Inspector General Schmitz:

I am writing to ask you to review the statutory authority and legal standing of the Total Information Awareness program being developed by the Defense Advance Research Projects Agency (DARPA).

I strongly support DARPA, and believe we must use our technological advantages to fight the war on terror, but I am concerned that this technology, if ever developed and used, could lead to violations of the Privacy Act, as well as other federal laws. I also share Senator Grassley's concern that military use of this technology might violate the Posse Comitatus Act which prohibits using military personnel in civilian law enforcement.

I think you will agree that the possibility for abuse of individual privacy rights is enormous. Therefore we must ensure this program is being conducted in accordance with federal law and that proper safeguards are in place to uphold the principles which underpin our free and open society.

I appreciate your attention to my request and look forward to your response.

Sincerely,

A handwritten signature in black ink that reads "Bill Nelson". The signature is written in a cursive, slightly slanted style.

## Appendix C. Inspector General of the Department of Defense Congressional Responses



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

JAN 17 2003

The Honorable Charles E. Grassley  
Chairman  
Committee on Finance  
United States Senate  
Washington, D. C. 20510-6200

Dear Mr. Chairman:

This is in further response to your letter of November 22, 2002, concerning the DoD research program entitled "Total Information Awareness (TIA) Program."

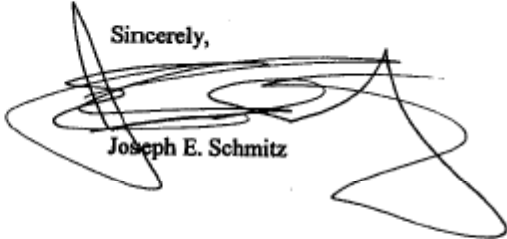
On December 20, 2002, Mr. Dean Zerbe and Mr. Matt Reed of your staff, along with Mr. Bob Nickel representing Senator Chuck Hagel, were briefed regarding the TIA program.

The TIA Program intends to use an overarching technical capability to link existing technologies for the purpose of gathering and combining data from existing databases to predict foreign terrorist activity. This capability could have a dual application to both the gathering of foreign intelligence and to domestic law enforcement (counter-terrorism). The primary application would be to provide our country and its deployed forces "defense in depth" by attempting to predict potential threat activity outside U.S. borders. The second application would be to use the technology to predict terrorist activity within the United States.

Enclosed is an initial response to the six questions contained in your letter of November 22, 2002. In addition, in response to your concerns and those of other Members of Congress, we initiated an audit on January 10, 2002, "to assess whether the proper controls are being included in the developmental contracts to ensure that the technology is properly managed and controlled when placed in an operational environment." The audit will include an examination of safeguards regarding the protection of privacy and civil liberties. The audit announcement letter is enclosed. You will be provided a copy of the final report when the audit is completed.

Please contact me or Mr. John R. Crane, Director, Office of Communications and Congressional Liaison, at (703) 604-8324, if you have any questions regarding this matter.

Sincerely,

  
Joseph E. Schmitz

Enclosures:  
As stated

cc: Honorable Max Baucus  
Ranking Member



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

January 10, 2003

MEMORANDUM FOR DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS  
AGENCY

SUBJECT: Audit of the DoD Total Information Awareness System  
(Project No. D2003CM-0056)

We plan to begin the subject audit in February 2003. The audit was initiated at the request of Senators Charles E. Grassley, Chuck Hagel, and Bill Nelson. Our objective will be to assess whether the proper controls are being included in the developmental contracts to ensure that the technology is properly managed and controlled when placed in an operational environment. The audit will also evaluate the management control program as it relates to the overall audit objective. We will fully consider recommendations from management on additional or revised audit objectives.

The audit will be performed primarily at the Defense Advanced Research Projects Agency and various Defense contractor locations. Other Government organizations to be visited may also be identified during the audit.

Please provide points of contact for this audit to Colonel William Kelley, (703)604-9312 (DSN 664-9312) (wkelley@dodig.osd.mil) or to Ms. Lisa Such, (703) 604-9284 (DSN 664-9284) (lsuch@dodig.osd.mil) within 30 days of the date of this memorandum.

A handwritten signature in cursive script that reads "David Steensma".

David K. Steensma  
Deputy Assistant Inspector General  
for Auditing

**Preliminary Responses to Questions from Senator Charles E. Grassley  
About the Total Information Awareness (TIA) Program**

***1. What is the statutory authorization for TIA?***

The TIA program is not authorized or funded as a separate line item in either the National Defense Authorization Act or the Department of Defense Appropriations Act. The TIA program, however, is identified as a program of the Defense Advanced Research Projects Agency (DARPA) in the Fiscal Year 2003 Budget Estimates, February 2002 (see attached).

***2. What are the parameters and scope of TIA?***

According to Dr. Anthony J. Tether, Director, DARPA, TIA is an IT system for combating terrorism.

***3. How was TIA selected to be funded?***

Dr. Tether reports that TIA was selected through their process of reviewing ideas they believe can be developed into useful technologies.

***4. How was Admiral Poindexter selected to head TIA?***

Dr. Tether selected Admiral John Poindexter, U.S. Navy (Retired). Admiral Poindexter was hired as a "Section 1101" appointee under 5 U.S.C. Sec. 3104 and Sec. 1101 of the Strom Thurmond Defense Authorization for Fiscal Year 1999 (P.L. 105-261).

***5. What coordination has the program had with Federal law enforcement officials? This should include details of what input was received prior to funding.***

Dr. Tether has advised of contacts with the Federal Bureau of Investigation (FBI), Foreign Terrorist Tracking Task Force, Department of Justice, and components of the Department of Homeland Security. DARPA officials note it is their understanding that the FBI is working on an MOU with DARPA for possible experimentation with TIA technology in the future.

***6. What protections are in place to ensure civil liberties are not violated?***

Dr. Tether has advised that part of the TIA project will focus on the development of privacy protections that do not currently exist, along with other advanced security and system hardening characteristics as part of the TIA program. The IG, DoD, audit will "assess whether the proper controls are being included in the developmental contracts to ensure that the technology is properly managed and controlled when placed in an operational environment." The audit will also assess the adequacy of computer security protections and human access protections intended to protect civil liberties.

UNCLASSIFIED

*Fiscal Year (FY) 2003 Budget Estimates*  
*February 2002*



*RESEARCH, DEVELOPMENT, TEST AND EVALUATION, DEFENSE-WIDE*  
*Volume I - Defense Advanced Research Projects Agency*

UNCLASSIFIED

Approved for Public Release  
.....

UNCLASSIFIED

RDT&E BUDGET ITEM JUSTIFICATION SHEET (R-2 Exhibit)		DATE
APPROPRIATION/BUDGET ACTIVITY RDT&E, Defense-wide BA3 Advanced Technology Development	R-1 ITEM NOMENCLATURE Command, Control and Communications Systems PE 0603760E, Project CCC-01	February 2002

- Project Genca II. (\$7,000 Million)
  - Design faster systems of humans and machines by assimilating new information technologies to operational agencies to meet asymmetric threats.
  - Develop tools for cognitive amplification by extending the ability of software to model current states, estimate plausible futures, support formal risk analysis, and provide for automated option planning. Supporting technology includes the use of intelligent agents, cognitive machine intelligence, associative memory, neural networks, pattern matching, Bayesian inference networks, and biologically inspired algorithms.
  - Develop tools for cross-agency collaboration designed to operate across existing hierarchical organizations while maintaining control and accountability. Areas under consideration will include: Knowledge Management; corporate memory; context-driven, declarative-policy enforcement; self-aware data; business rules; self-governance; and automated planning.
- Total Information Awareness (TIA). (\$10,000 Million)
  - Initiate development of architectures for large-scale counter-terrorism database.
  - Develop novel methods for populating database from existing sources.
  - Develop new models, algorithms, methods, tools and techniques for analyzing and correlating information in the database.
- Advanced Sensor/Strike Battle Manager. (\$5,000 Million)
  - Build models, plan authoring tools, and planning algorithms to plan strike missions using air platforms carrying both sensors and strike weapons.
  - Incorporate a capability to manage shoot-look-shoot engagement strategies supported by multiple platforms.
- Advanced Ground Tactical Battle Manager. (\$5,000 Million)
  - Build situation estimation, situation assessment, and tactical plan generation tools to generate and update, continuously, plans for tactical ground combat.
  - Incorporate a capability to create and modify new tactics in response to evolving enemy capabilities and differing operational environments.



INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

JAN 17 2003

The Honorable Chuck Hagel  
United States Senate  
Washington, D. C. 20510-2705

Dear Senator Hagel:

This is in further response to your letter of December 2, 2002, regarding the Total Information Awareness (TIA) Program.

On December 20, 2002, Mr. Bob Nickel of your staff, along with Mr. Dean Zerbe and Mr. Matt Reed representing Senator Charles E. Grassley, were briefed to provide an interim response to your concerns.

The TIA Program intends to use an overarching technical capability to link existing technologies for the purpose of gathering and combining data from existing databases to predict foreign terrorist activity. This capability could have a dual application to both the gathering of foreign intelligence and to domestic law enforcement (counter-terrorism). The primary application would be to provide our country and its deployed forces "defense in depth" by attempting to predict potential threat activity outside U.S. borders. The second application would be to use the technology to predict terrorist activity within the United States.

In your letter of December 2, 2002, you raised a concern that the separation of responsibilities between the military and domestic police functions be maintained as specified in the Posse Comitatus Act. In response to your concerns and those of Senator Charles E. Grassley and other Members of Congress, we initiated an audit on January 10, 2002, "to assess whether the proper controls are being included in the developmental contracts to ensure that the technology is properly managed and controlled when placed in an operational environment." The audit will include an examination of safeguards regarding the protection of privacy and civil liberties. The audit announcement letter is enclosed. You will be provided a copy of the final report when the audit is completed.

Please contact me or Mr. John R. Crane, Director, Office of Communications and Congressional Liaison, at (703) 604-8324, if you have any questions regarding this matter.

Sincerely,



Joseph E. Schmitz

Enclosure:  
As stated





INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
400 ARMY NAVY DRIVE  
ARLINGTON, VIRGINIA 22202-4704

JAN 17 2003

The Honorable Bill Nelson  
United States Senate  
Washington, D. C. 20515-0905

Dear Senator Nelson:

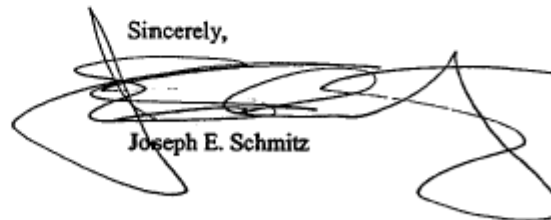
This is in further response to your letter of December 13, 2002, concerning the DoD research program entitled, "Total Information Awareness (TIA) Program."

The TIA Program intends to use an overarching technical capability to link existing technologies for the purpose of gathering and combining data from existing databases to predict foreign terrorist activity. This capability could have a dual application to both the gathering of foreign intelligence and to domestic law enforcement (counter-terrorism). The primary application would be to provide our country and its deployed forces "defense in depth" by attempting to predict potential threat activity outside U.S. borders. The second application would be to use the technology to predict terrorist activity within the United States.

In your letter of December 13, 2002, you raised concerns that the technology, if developed and used, could lead to violations of the Privacy Act, the Posse Comitatus Act, as well as other federal laws. In response to your concerns and those of Senator Charles E. Grassley and other Members of Congress, we initiated an audit on January 10, 2002, "to assess whether the proper controls are being included in the developmental contracts to ensure that the technology is properly managed and controlled when placed in an operational environment." The audit will include an examination of safeguards regarding the protection of privacy and civil liberties. The audit announcement letter is enclosed. You will be provided a copy of the final report when the audit is completed.

Please contact me or Mr. John R. Crane, Director, Office of Communications and Congressional Liaison, at (703) 604-8324, if you have any questions regarding this matter.

Sincerely,



Joseph E. Schmitz

Enclosure:  
As stated

---

## Appendix D. TIA Subsystems

**Genisys.** The Genisys Program seeks to produce technology that can integrate and broaden databases as well as other information sources and support effective intelligence analysis aimed at preventing terrorist attacks. Projected funding for FY 2003 through FY 2005: \$22.8 million.

**Genisys Privacy Protection.** The Genisys Privacy Protection program aims to provide security with privacy by controlling access to unauthorized information, enforcing laws and policies, and ensuring that any misuse of data can be quickly detected and addressed. Projected funding for FY 2003 through FY 2005: \$13.8 million.

**EELD (Evidence Extraction and Link Discovery).** The EELD program is intended to automatically extract evidence about relationships among people, organizations, places, and things from unstructured textual data, such as intelligence messages or news reports, which are the starting points for further analysis. Projected funding for FY 2002 through FY 2005: \$44.6 million.

**SSNA (Scalable Social Network Analysis).** The SSNA algorithm program will help distinguish potential terrorist cells based on their patterns of interactions from legitimate groups of people and identify when a terrorist group plans to execute an attack. Projected funding for FY 2003 through FY 2005: \$7.4 million.

**MinDet (Misinformation Detection).** The MinDet Program will develop the ability to detect intentional misinformation and to detect inconsistencies in open source data with regard to known facts and adversaries' goals. Other potential uses include the ability to detect misleading information on various Government forms such as visa applications that would suggest that a further investigation may be warranted. Projected funding for FY 2003 through FY 2005: \$20 million.

**HumanID (Human Identification at a Distance).** The HumanID program seeks to develop technologies that can detect, recognize, and identify humans at a distance. Projected funding for FY 2002 through FY 2004: \$32.2 million.

**ARM (Activity, Recognition and Monitoring).** The ARM Program seeks to develop an automated capability that can reliably capture, identify, and classify human activities in surveillance environments. Projected funding for FY 2004 through FY 2005: \$15 million.

**NGFR (Next-Generation Face Recognition).** The NGFR Program seeks to develop a new generation of facially based biometrics. Projected funding for FY 2004 through FY 2005: \$17.1 million.

**GENOA II.** GENOA II will provide for TIA collaborative reasoning tools that will enable distributed teams of analysts and decision-makers to more effectively use the information resources available. Projected funding for FY 2003 through FY 2005: \$50.8 million.

**WAE (Wargaming the Asymmetric Environment).** The WAE Program seeks to develop automated predictive models that are tuned to the behavior of specific foreign

---

terrorist groups and will facilitate development of more effective force protection and intervention strategies. The WAE Program predates both the IAO and the TIA program. Projected funding for FY 2002 through FY 2004: \$41.7 million.

**RAW (Rapid Analytical Wargaming).** The RAW Program will develop an analytical simulation that supports U.S. readiness across analytical, operational, and training domains for asymmetric and symmetric missions. Projected funding for FY 2004 through FY 2005: \$16.9 million.

**FutureMAP (Futures Markets Applied to Prediction).** The FutureMAP Program was designed to provide DoD with market-based techniques for avoiding surprise and predicting future events. DoD cancelled the FutureMAP program in July 2003. Projected funding for FY 2004 through FY 2005: \$8 million.

**EARS (Effective, Affordable, Reusable Speech-to-Text).** The EARS technology aims to create effective speech-to-text technology for human to human speech, focusing on broadcasts and telephone conversations to produce technology that can be rapidly translated to many languages and a number of applications. No costs or milestones dates were available.

**TIDES (Translingual Information Detection, Extraction, and Summarization).** TIDES aims to make it possible for English speakers to find and interpret needed information quickly and effectively, regardless of language or medium. Milestone dates were given but no costs were available.

**GALE (Global Autonomous Language Exploitation).** GALE aims to make it possible for machines to discover critical foreign intelligence information in vast quantities of human language, both speech and text, from around the globe, delivering it in actionable form to military operators and intelligence analysts without requiring them to issue specific requests. Projected funding for FY 2002 through FY 2005: \$156.7 million.

**Bio-ALIRT (Bio-Event Advanced Leading Indicator Recognition Technology).** The objective of the Bio-ALIRT Program is to develop technology for early detection of a covert biological attack. The Bio-ALIRT Program predates both the IAO and the TIA program. Projected funding for the FY 2002 through FY 2004: \$33.4 million.

---

## **Appendix E. Report Distribution**

### **Office of the Secretary of Defense**

Under Secretary of Defense for Acquisition, Technology, and Logistics  
Director, Defense Research and Engineering  
Under Secretary of Defense for Intelligence  
Assistant Secretary of Defense Networks and Information Integration  
Deputy Chief Financial Officer  
Deputy Comptroller (Program/Budget)  
Assistant to the Secretary of Defense (Intelligence Oversight)

### **Department of the Army**

Auditor General, U.S. Army Audit Agency  
Inspector General, Department of the Army  
Commander, U.S. Army Intelligence and Security Command

### **Department of the Navy**

Naval Inspector General  
Naval Audit Service  
Department of the Navy, Superintendent Naval Postgraduate School

### **Department of the Air Force**

Auditor General, Department of the Air Force

### **Unified Command**

Commander, U.S. Joint Forces Command

### **Other Defense Organizations**

Director, Defense Advanced Research Projects Agency  
Director, Washington Headquarters Service  
Director, Defense Privacy Office  
Director, Defense Contract Audit Agency  
Defense Contract Management Agency  
Director, Defense Information Systems Agency  
Defense Intelligence Agency  
Director, Defense Logistics Agency  
Defense Systems Management College  
Inspector General, National Geospatial-Intelligence Agency  
National Security Agency

---

## **Non-Defense Federal Organization**

Office of Management and Budget

## **Congressional Committees and Subcommittees, Chairman and Ranking Minority Member**

Senate Committee on Appropriations

Senate Subcommittee on Defense, Committee on Appropriations

Senate Committee on Armed Services

Senate Committee on Governmental Affairs

Senate Subcommittee on Emerging Threats and Capabilities Committee on Armed Services

Senate Select Committee on Intelligence

Senate Subcommittee on Terrorism Unconventional Threats and Capabilities

Senate Permanent Select Committee on Intelligence

House Committee on Appropriations

House Subcommittee on Defense, Committee on Appropriations

House Committee on Armed Services

House Committee on Government Reform

House Subcommittee on National Security Emerging Threats and International Relations

House Subcommittee on Government Efficiency and Financial Management

House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census

Honorable Charles E Grassley, U.S. Senate

Honorable Chuck Hagel, U.S. Senate

Honorable Bill Nelson, U. S. Senate



# Director, Defense Research and Engineering Comments

Final Report  
Reference



DIRECTOR OF DEFENSE RESEARCH AND ENGINEERING  
3030 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-3030

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

THROUGH: DIRECTOR, ACQUISITION RESOURCES AND ANALYSIS

7/8  
12/3/03

SUBJECT: Comment on Draft Department of Defense Inspector General (DoD IG) Report on  
Terrorism Information Awareness (TIA) Program (Project No. D2003CM-0056)

I have reviewed the DoD IG draft report and offer the following comments for consideration and inclusion in preparation for follow-up activities:

I concur with the importance of Privacy Impact Assessments and acknowledge that TIA represents a technology area meriting special measures to protect the privacy of U.S. citizens. Decisions made by DARPA early in project conceptualization, subsequent studies undertaken by DARPA and on-going technology review panels constitute effective and appropriate measures to protect privacy during the technology development and evaluation process. Formal Privacy Impact Assessments focused on specific end-user applications should precede all transitions to operational employment of TIA tools.

The issue advanced by the draft IG report is the implied requirement for anticipatory policy enforcement, i.e., anticipating end uses of developmental technical tools. By charter, DARPA is an advanced research technology organization. As stated in the DoD IG report, the decision to employ intelligence and synthetic data during the project development phase reflects deliberate consideration of privacy concerns at a level appropriate for a research effort. Certification of compliance via a formal privacy impact assessment process would more effectively protect U.S. citizens when undertaken in the context of end-user applications.

The DoD IG report should conclude that the TIA project has not, in fact, violated privacy policies of the United States. Presently this is unstated. The draft report does however serve a useful purpose in discussing privacy concerns and protective processes that should be addressed during transition of research projects to domestic applications. The report would be even more useful as a positive roadmap for transition of such advanced development efforts rather than a censure prior to complete operational specification. The draft report states that the "Office of Management and Budget (OMB) is responsible for issuing guidance specifying the required contents of a privacy impact statement". At the time of your draft report guidance had not been disseminated. In the absence of guidance, DARPA restricted developmental efforts to intelligence and synthetic databases, subsequently formed review boards, and implemented DARPA research into privacy safeguards. We believe these actions constitute effective efforts to protect citizen rights while developing technologies that could significantly improve our nation's countermeasures against terrorism.

Responses to the specific recommendations advanced in the draft report follow:



**DoDIG Recommendation 1:** Perform a Privacy Impact Assessment before Terrorism Information Awareness type technology continues.

**ODUSD(AT&L) Response:** Concur with comments. The USD(AT&L) established additional oversight mechanisms through the Internal Oversight Board and the Outside Advisory Committee Board (Technology and Privacy Advisory Committee - TAPAC). These processes are equivalent to privacy act assessments. (Note: The TAPAC convened five times in the past year, vice three sessions cited on page 9 of the draft report.) On-going review of TIA projects provides effective assessments of data employment and knowledge products during the research and technology development phase. Formal Privacy Impact Assessments should be conducted, reviewed and approved before authorizing use of TIA tools in operational applications.

**DoDIG Recommendation 2:** Appoint a Privacy Ombudsman or equivalent official specifically for the development of Terrorism Information Awareness type technology who will ensure that individual Terrorism Information Awareness type technology are scrutinized from a privacy perspective as a means of safeguarding individual privacy.

**ODUSD(AT&L) Response:** Concur.

My points of contact for this action are Mr. Tim McClees at 703-692-4592 and CAPT Mike Knollmann at 703-695-5036.



Ronald M. Segal



# Director, Defense Advanced Research Projects Agency Comments

Final Report  
Reference



DEFENSE ADVANCED RESEARCH PROJECTS AGENCY  
3701 NORTH FAIRFAX DRIVE  
ARLINGTON, VA 22203-1714

NOV 10 2003

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE  
ATTN: PROGRAM DIRECTOR, CONTRACT MANAGEMENT DIRECTORATE

SUBJECT: Comment on Draft Report on Terrorism Information Awareness Program (Project #D2003CM-0056)

You state that the report was accomplished in response to letters from U.S. Senators which are attached in Appendix B. The letters from the Senators express concern that DARPA was developing Domestic Law Enforcement for which we had no statutory right to do so.

Your report does not answer these concerns. The report does state that TIA was not being developed for Domestic Law Enforcement (Page 2, DoD Partners in TIA Experiments), and even goes so far to state that DARPA had not established any formal agreement outside of DoD (Page 2, Other Federal Agency Participation in TIA Experiments).

We recommend that the report explicitly state that DARPA was not developing a system for Domestic Law Enforcement. The fact that it could be used by Law Enforcement was acknowledged by DARPA in its February 2003 Strategic Plan and the May 2003 report required by the Wyden Amendment. In addition, the plan and congressional report stated that any use would first have to be approved by Congress and other authorities.

The report on page 4 states that "DARPA did not implement the best business practice of performing a privacy impact assessment." Yet on page 6 the report states that "The requirement to perform a privacy impact assessment does not apply to systems that involve intelligence activities and because DARPA was using intelligence and synthetic in the development and testing of TIA, a privacy impact assessment was not require."

We recommend that it be made very clear on page 4 and wherever the report is summarized, that a privacy impact assessment was not required to be done by DARPA because the development of TIA was not using data requiring such an assessment.

We believe however that a statement that any organization deciding to use TIA products should do a privacy impact assessment if applicable is warranted. In the case of the current development partners, a privacy impact statement would not be required. But if a Law Enforcement organization wanted to use TIA products, they would be required to perform a privacy impact assessment.

We have provided comments on an earlier draft and find them still applicable. However the above comments are in our opinion significant and could lead to a misleading report if our recommendations are not accepted.

Sincerely,

Anthony J. Tether  
Director

Revised  
See  
Appendix C

## **Team Members**

The Contract Management Directorate, Office of the Deputy Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Colonel William J. Kelley, U.S. Army Reserve

Lisa M. Such

Pamela S. Varner

Sharon Dworkin

Justin Husar