Report to Congress regarding the Terrorism Information Awareness Program

In response to Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division M, § 111(b)

Executive Summary

May 20, 2003

Terrorism Information Awareness Program

Preface

The Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, Division M, § 111(b) provides for the submission of a report to Congress, within 90 days of the President's signing the law, regarding the Total Information Awareness program, now called the Terrorism Information Awareness (TIA) program, a Defense Advanced Research Projects Agency (DARPA) research and development program initiated in the aftermath of the September 11, 2001 terrorist attacks on New York and Washington.

Executive Summary

The Defense Advanced Research Projects Agency (DARPA) is charged with conducting research and development for the Department of Defense (DoD). By doing so, DARPA furnishes DoD with leading-edge technologies to help the department execute its critical national security mission. DARPA often produces prototype systems for conducting experiments that address the urgent needs of DoD. If successful and as appropriate, such prototype systems would be transitioned into operational use by executing agencies of the government.

Terrorism Information Awareness (TIA)[1] is such a prototype system/network. It is a research and development program that will integrate advanced collaborative and decision support tools; language translation; and data search, pattern recognition, and privacy protection technologies into an experimental prototype network focused on combating terrorism through better analysis and decision making. If successful, and if deployed, this program of programs would provide decision- and policy-makers with advance actionable information and knowledge about terrorist planning and preparation activities that would aid in making informed decisions to prevent future international terrorist attacks against the United States at home or abroad. In short, DoD's aim in TIA is to seek to make a significant leap in technology to help those working to "connect the dots" of terrorist-related activity. A TIA-like system/network could provide the defense and intelligence communities with tools and methods to solve many of the problems that have been identified in the aftermath of the attacks against the United States on September 11, 2001,[2] and that are related to improving information analysis in our continuing war against terrorism.

[1] Previously known as Total Information Awareness, this name created in some minds the impression that TIA was a system to be used for developing dossiers on U.S. citizens. That is not DoD's intent in pursuing this program. Rather, DoD's purpose in pursuing these efforts is to protect U.S. citizens by detecting and defeating foreign terrorist threats before an attack. To make this objective absolutely clear, DARPA has changed the program name to Terrorism Information Awareness.

[2] Final Report of the Joint SSCI/HPSCI Inquiry into the Events of 9/11/01 dated Dec 10, 2002.

DoD's TIA research and development is aimed at providing capabilities to users/analysts/operators to addresses a perennial array of problems that have beset analysis of complex threats, including sharing data across agency boundaries and exploiting both classified and unclassified information, in a more systematic fashion.

These problems exist in part because of a lack of applied technology to aid the human processes. Today, the amount of information that needs to be considered far exceeds the capacity of the un-aided humans in the system. Adding more people is not necessarily the solution. DoD believes that there is a need to provide a much more systematic, methodological approach that automates many of the lower-level data manipulation tasks that can be done well by machines guided by human users. Such an approach would, in turn, allow users more time for higher-level analysis that depends critically on a human's unique cognitive skills.

TIA is one of several research and development programs in DARPA's Information Awareness Office (IAO), which was established in January 2002. In the aftermath of the September 11 terrorist attacks, DARPA formed IAO in part to bring together, under the leadership of one technical office director, several existing DARPA programs focused on applying information technology to combat terrorist threats. DARPA also recognized that new programs would be needed to fully address the technology requirements of a complete prototype system/network to respond to the particular demands of the terrorist threat. DARPA envisions TIA as the system/ network-level integration program while other IAO programs are designed to furnish technologies and components that compose the overall program. As conceived by DARPA, TIA would integrate these technologies and provide some or all of them to various organizations for experiments, while assessing the system's utility in various operationally relevant contexts.

The TIA research and development program began in FY 2003. Funding for FY 2003 through FY 2005 as proposed in the FY 2004 President's Budget submission is $53,752,000. A number of organizations in the DoD and Intelligence Community have shown great interest in working with the TIA program to test and evaluate technologies.

DARPA provides a system/network infrastructure and concepts; software analytical tools; software installation; training; software performance evaluation; and integration and evaluation of user comments on modifications and additions to the software. Participating organizations from DoD and the Intelligence Community provide facilities and personnel to evaluate these products and use data currently available to them under existing laws, regulations and policies.

Five major investigation threads are currently being pursued as a part of TIA and are driving much of the development and experimental activity in the TIA program. These five threads are: secure collaborative problem solving, structured discovery with security, link and group understanding, context aware visualization, and decision making with corporate memory.

- **Secure Collaborative Problem Solving.** A collaborative environment is sought that would enable ad hoc groups to quickly form within and across agency boundaries to bring relevant data, diverse points of view, and experience together to solve the complex problems associated with countering terrorism.

- **Structured Discovery with Sources and Methods Security.** A wide range of intelligence data, both classified and open source, may need to be searched to find relevant information for understanding the terrorist intent. DARPA believes that to have any hope of making sense of this wide range of data, a more structured and automated way of approaching the problem is needed.

- **Link and Group Understanding.** One of the characteristics of the terrorist threat is that terrorist organizational structures are not well understood and are purposefully designed to conceal their connections and relationships. IAO is researching software that can discover linkages among people, places, things, and events related to possible terrorist activity.

- **Context Aware Visualization. DARPA believes that b**etter ways are needed to visualize information than text-based lists, tables, and long passages of unstructured text. Such visualization concepts should respond to a broad range of potential users with wholly different roles and responsibilities.

- **Decision Making with Corporate Memory.** Decision-makers must consider a full range of possible options to deal with complex asymmetric threats, particularly in light of rapidly changing circumstances. DARPA's activities in this area are premised on the view that understanding how certain decisions played out in the past is critical to formulating current decision options.

The TIA program is a research and development project. The program is integrating and testing information technology tools. DARPA affirms that TIA's research and testing activities are only using data and information that is either (a) foreign intelligence and counter intelligence information legally obtained and usable by the Federal Government under existing law, or (b) wholly synthetic (artificial) data that has been generated, for research purposes only, to resemble and model real-world patterns of behavior .

The Department of Defense, which is responsible for DARPA, has expressed its full commitment to planning, executing, and overseeing the TIA program in a manner that protects privacy and civil liberties. Safeguarding the privacy and the civil liberties of Americans is a bedrock principle. DoD intends to make it a central element in the Department of Defense's management and oversight of the TIA program.

The Department of Defense's TIA research and development efforts address both privacy and civil liberties in the following ways:

- The Department of Defense must fully comply with the laws and regulations governing intelligence activities and all other laws that protect the privacy and constitutional rights of U.S. persons.

- As an integral part of its research, the TIA program itself is seeking to develop new technologies that will safeguard the privacy of U.S. persons.

- TIA's research and testing activities are conducted using either real intelligence information that the federal government has already legally obtained, or artificial synthetic information that, ipso facto, does not implicate the privacy interests of U.S. persons.

The report does not recommend any changes in statutory laws, but instead contemplates that any deployment of TIA's search tools may occur only to the extent that such a deployment is consistent with current law. Accordingly, the report specifically notes that the strictures of current law protecting certain categories and sources of information may well constrain or (as a logistical matter) completely preclude deployment of TIA search tools with respect to such data.

Moreover, to the extent that TIA research and development technology is ever applied to data sources that contain information on U.S. persons, the privacy issues raised by these tools are significant ones that will require careful and serious examination. Because TIA is still largely in the research stage, any analysis of these issues is necessarily tentative and preliminary. Several factors would need to be considered in evaluating TIA's suitability for deployment in particular contexts.

- The *efficacy and accuracy* of TIA's search tools must be stress-tested and demonstrated. The tools must be shown to be sufficiently precise and accurate – i.e., a search query results in *only* that information that is responsive to the query. DARPA has expressed its commitment to the necessary testing to ensure the technological accuracy of TIA's search tools.

- It is critical that there be *built-in operational safeguards* to reduce the opportunities for abuse. DARPA is already researching whether and how it may be able to build in controls that, at an architectural level, would govern the TIA program tools. Among the controls being researched are automated audit trails to document who accessed the system and how it was used during the session; anonymization of sources of data and of the persons mentioned in the underlying data, so that these data could not be revealed unless it is lawful and warranted; selective revelation of data, so that additional permissions would need to be obtained in order to receive additional data; and rigorous access controls and permissioning techniques. TIA's ultimate suitability for particular purposes will depend heavily upon DARPA's success on these technological issues.

- It will also be essential to ensure that *substantial security measures* are in place to protect these tools from unauthorized access by hackers or other intruders. Some of these measures must be built-in at the architectural level; others will involve the adoption of policies that prescribe who may have access, for what purposes, and in what manner.

- Any agency contemplating deploying TIA tools for use in particular contexts will be required first to conduct a *pre-deployment legal review*. In this regard, the DoD General Counsel has directed each operational component within DoD that hosts TIA technologies to prepare a substantive legal review that examines the relationship between that component and TIA, and analyzes the legal issues raised by the underlying program to which the TIA tools will be applied. The General Counsel has advised that all such relationships should be documented in a memorandum of agreement to ensure the relationship is clearly understood by all parties. The DCI's General Counsel is taking comparable steps with respect to elements of the Intelligence Community, and the Department of Justice would do so if it ever decides to deploy any TIA technology.

- There will be a need for any user agency to adopt policies establishing *effective oversight* of the actual use and operation of the system before it is deployed in particular contexts. There must be clear and effective accountability for misuse of the system.

As DARPA endeavors to achieve these technological developments, the Secretary of Defense will, as an integral part of oversight of TIA research and development, continue to assess emerging potential privacy and civil liberties impacts through an oversight board composed of senior representatives from DoD and the Intelligence Community, and chaired by the Under Secretary of Defense (Acquisition, Technology and Logistics). The Secretary of Defense will also receive advice on legal and policy issues, including privacy, posed by TIA research and development from a Federal Advisory Committee composed of outside experts.

The Department of Defense has expressed its intention to address privacy and civil liberties issues squarely as they arise, in specific factual and operational contexts and in full partnership with other Executive Branch agencies and the Congress. The protection of privacy and civil liberties is an integral and paramount goal in the development of counterterrorism technologies and in their implementation. If these technologies can be developed, the privacy and civil liberties issues noted above would have to be carefully considered and resolved in advance of deployment.