



WIKIPEDIA
The Free Encyclopedia

[Main page](#)
[Contents](#)
[Featured content](#)
[Current events](#)
[Random article](#)
[Donate to Wikipedia](#)
[Wikipedia store](#)

[Interaction](#)

[Help](#)
[About Wikipedia](#)
[Community portal](#)
[Recent changes](#)
[Contact page](#)

[Tools](#)

[What links here](#)
[Related changes](#)
[Upload file](#)
[Special pages](#)
[Permanent link](#)
[Page information](#)
[Wikidata item](#)
[Cite this page](#)

[Print/export](#)

[Create a book](#)
[Download as PDF](#)
[Printable version](#)

[Languages](#)

[Català](#)
[Deutsch](#)
[Français](#)
[Italiano](#)
[Suomi](#)
[Svenska](#)

[Edit links](#)

Article [Talk](#)

Read [Edit](#) [View history](#)



Wiki Loves Monuments: Photograph a monument, help Wikipedia and win!

[Learn more](#)

Information Awareness Office

From Wikipedia, the free encyclopedia

The **Information Awareness Office** (**IAO**) was established by the United States [Defense Advanced Research Projects Agency](#) (DARPA) in January 2002 to bring together several DARPA projects focused on applying [surveillance](#) and information technology to track and monitor terrorists and other [asymmetric threats](#) to U.S. [national security](#) by achieving "[Total Information Awareness](#)" (TIA).^{[4][5][6]}

This was achieved by creating enormous computer databases to gather and store the personal information of everyone in the United States, including personal e-mails, social networks, credit card records, phone calls, medical records, and numerous other sources, without any requirement for a search warrant.^[7] This information was then analyzed to look for suspicious activities, connections between individuals, and "threats".^[8] Additionally, the program included funding for [biometric surveillance](#) technologies that could identify and track individuals using surveillance cameras, and other methods.^[8]

Following public criticism that the development and deployment of this



Information Awareness Office seal^{[1][2]}
(motto: *lat. scientia est potentia* – *knowledge is power*^[3])

Part of a series on

Global surveillance



Disclosures

[Origins](#) · [Pre-2013](#) · [2013–present](#) · [Reactions](#)

Systems

[XKeyscore](#) · [PRISM](#) · [ECHELON](#) · [Carnivore](#) · [Dishfire](#) · [Stone Ghost](#) · [Tempora](#) · [Frenchelton](#) · [Fairview](#) · [MYSTIC](#) · [DCSN](#) · [Boundless Informant](#) · [Bullrun](#) · [Pinwale](#) · [Stingray](#) · [SORM](#) · [RAMPART-A](#)

Agencies

[NSA](#) · [BND](#) · [CNI](#) · [ASIO](#) · [DGSE](#) · [Five Eyes](#) · [FSB](#) · [MSS](#)

People

[Michael S. Rogers](#) · [Keith Alexander](#) · [James Bamford](#) · [James Clapper](#) ·

technology could potentially lead to a [mass surveillance](#) system, the IAO was defunded by [Congress](#) in 2003. However, several IAO projects continued to be funded and merely run under different names, as revealed by [Edward Snowden](#) during the course of the [2013 mass surveillance disclosures](#).^{[5][6][9][10][11][12]}

Contents [hide]

- 1 [History](#)
- 2 [Research](#)
 - 2.1 [Human Identification at a Distance \(HumanID\)](#)
 - 2.2 [Evidence Extraction and Link Discovery](#)
 - 2.3 [Genisys](#)
 - 2.4 [Scalable Social Network Analysis](#)
 - 2.5 [Futures Markets Applied to Prediction \(FutureMAP\)](#)
 - 2.6 [TIDES](#)
 - 2.7 [Genoa / Genoa II](#)
 - 2.8 [Wargaming the Asymmetric Environment \(WAE\)](#)
 - 2.9 [Effective Affordable Reusable Speech-to-text \(EARS\)](#)
 - 2.10 [Babylon](#)
 - 2.11 [Bio-Surveillance](#)
 - 2.12 [Communicator](#)
- 3 [Components of TIA projects that continue to be developed](#)
- 4 [Media coverage and criticism](#)
- 5 [See also](#)
- 6 [References](#)
- 7 [Further reading](#)
- 8 [External links](#)
 - 8.1 [Media coverage](#)
 - 8.2 [Academic articles](#)
 - 8.3 [Critical views](#)
 - 8.4 [Proponent views](#)

[Duncan Campbell](#) · [Edward Snowden](#) · [Russ Tice](#) · [George W. Bush](#) · [Barack Obama](#) · [Julian Assange](#)

Places

[The Doughnut](#) · [Fort Meade](#) · [Menwith Hill](#) · [Pine Gap](#) · [Southern Cross Cable](#) · [Utah Data Center](#) · [Bad Aibling Station](#) · [Dagger Complex](#)

Laws

[Five Eyes \(UKUSA Agreement · Lustre\)](#) · [U.S. \(USA Freedom Act · FISA amendments\)](#) · [EU \(Data Retention Directive · Data Protection Directive\)](#)

Proposed changes

[U.S. \(FISA Improvements Act · Other proposals\)](#)

Concepts

[Mass surveillance](#) · [Culture of fear](#) · [Secure communication](#) · [SIGINT](#) · [Call detail record](#) · [Surveillance issues in smart cities](#)

Related topics

[Espionage](#) · [Intelligence agency](#) · [Cryptography \(Tor · VPNs · TLS\)](#) · [Human rights \(Privacy · Liberty\)](#) · [Satellites](#) · [Stop Watching Us](#) · [Nothing to hide argument](#)

V · T · E

History [[edit](#)]

The IAO was established after Admiral [John Poindexter](#), former [United States National Security Advisor](#) to President [Ronald Reagan](#), and SAIC executive [Brian Hicks](#) approached the [US Department of Defense](#) with the idea for an information awareness program after the attacks of [September 11, 2001](#).^[11]

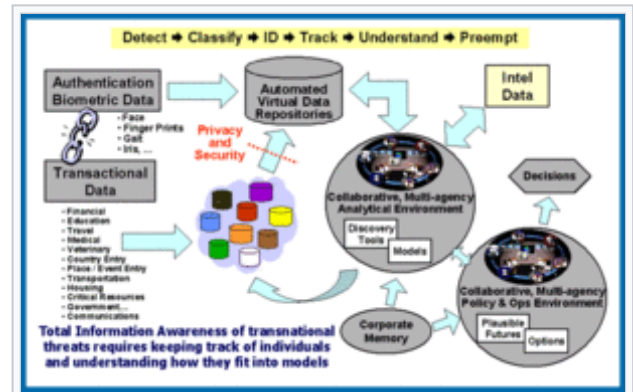


Diagram of Total Information Awareness system, taken from official (decommissioned) Information Awareness Office website (click to enlarge)

Poindexter and Hicks had previously worked together on intelligence-technology programs for the Defense Advanced Research Projects Agency. DARPA agreed to host the program and appointed Poindexter to run it in 2002.

The IAO began funding research and development of the [Total Information Awareness](#) (TIA) Program in February 2003 but renamed the program the *Terrorism* Information Awareness Program in May that year after an adverse media reaction to the program's implications for public surveillance. Although TIA was only one of several IAO projects, many critics and news reports conflated TIA with other related research projects of the IAO, with the result that TIA came in popular usage to stand for an entire subset of IAO programs.

The TIA program itself was the "systems-level" program of the IAO that intended to integrate information technologies into a prototype system to provide tools to better detect, classify, and identify potential terrorists with the goal to increase the probability that authorized agencies of the United States could preempt adverse actions.^[13]

As a systems-level program of programs, TIA's goal was the creation of a "counter-terrorism information architecture" that integrated technologies from other IAO programs (and elsewhere, as appropriate). The TIA program was researching, developing, and integrating technologies to virtually aggregate data, to follow subject-oriented link analysis, to develop descriptive and predictive models through data mining or human hypothesis, and to apply such models to additional datasets to identify terrorists and terrorist groups.^[13]

Among the other IAO programs that were intended to provide TIA with component data aggregation and automated analysis technologies were the Genisys, Genisys Privacy Protection, Evidence Extraction and Link Discovery, and Scalable Social Network Analysis programs.

On August 2, 2002, Dr. Poindexter gave a speech at DARPAtech 2002 entitled "Overview of the Information Awareness Office"^[14] in which he described the TIA program.

In addition to the program itself, the involvement of Poindexter as director of the IAO also raised concerns among some, since he had been earlier convicted of lying to Congress and altering and destroying documents pertaining to the [Iran-Contra](#)

[Affair](#), although those convictions were later overturned on the grounds that the testimony used against him was protected.

On January 16, 2003, Senator [Russ Feingold](#) introduced legislation to suspend the activity of the IAO and the Total Information Awareness program pending a Congressional review of privacy issues involved.^[15] A similar measure introduced by Senator [Ron Wyden](#) would have prohibited the IAO from operating within the United States unless specifically authorized to do so by Congress, and would have shut the IAO down entirely 60 days after passage unless either the Pentagon prepared a report to Congress assessing the impact of IAO activities on individual privacy and civil liberties or the President certified the program's research as vital to national security interests. In February 2003, Congress passed legislation suspending activities of the IAO pending a Congressional report of the office's activities (Consolidated Appropriations Resolution, 2003, No.108–7, Division M, §111(b) [signed Feb. 20, 2003]).

In response to this legislation, [DARPA](#) provided Congress on May 20, 2003 with a report on its activities.^[16] In this report, IAO changed the name of the program to the *Terrorism Information Awareness Program* and emphasized that the program was not designed to compile dossiers on US citizens, but rather to research and develop the tools that would allow authorized agencies to gather information on terrorist networks. Despite the name change and these assurances, the critics continued to see the system as prone to potential misuse or abuse.^[13]

As a result, House and Senate negotiators moved to prohibit further funding for the TIA program by adding provisions to the Department of Defense Appropriations Act, 2004^[17] (signed into law by President Bush on October 1, 2003). Further, the Joint Explanatory Statement included in the conference committee report specifically directed that the IAO as program manager for TIA be terminated immediately.^[18]

Research [\[edit \]](#)

IAO research was conducted along five major investigative paths: secure collaboration problem solving; structured discovery; link and group understanding; context aware visualization; and decision making with corporate memory.

Among the IAO projects were:

Human Identification at a Distance (HumanID) [\[edit \]](#)

The **Human Identification at a Distance (HumanID)** project developed automated [biometric](#) identification technologies to detect, recognize and identify humans at great distances for "force protection", crime prevention, and "homeland security/defense" purposes.^[19]



Its goals included programs to:[19]

Diagram (from official IAO site) describing capabilities of the "Human Identification at a Distance (HumanID)" project [19]

- Develop algorithms for locating and acquiring subjects out to 150 meters (500 ft) in range.
- Fuse face and [gait](#) recognition into a 24/7 human identification system.
- Develop and demonstrate a human identification system that operates out to 150 meters (500 ft) using visible imagery.
- Develop a low power millimeter wave radar system for wide field of view detection and narrow field of view gait classification.
- Characterize gait performance from video for human identification at a distance.
- Develop a multi-spectral infrared and visible face recognition system.

Evidence Extraction and Link Discovery [edit]

Evidence Extraction and Link Discovery (EELD) development of technologies and tools for automated discovery, extraction and linking of sparse evidence contained in large amounts of classified and unclassified data sources (such as phone call records from the [NSA call database](#), internet histories, or bank records).[20]

EELD was designed to design systems with the ability to extract data from multiple sources (e.g., text messages, social networking sites, financial records, and web pages). It was to develop the ability to detect patterns comprising multiple types of links between data items or people communicating (e.g., financial transactions, communications, travel, etc.).[20]

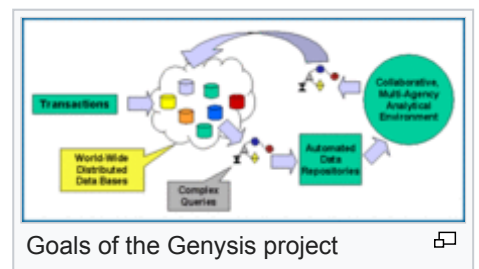
It is designed to link items relating potential "terrorist" groups and scenarios, and to learn patterns of different groups or scenarios to identify new organizations and emerging threats.[20]

Genisys [edit]

Genisys aimed at developing technologies which would enable "ultra-large, all-source information repositories".[21]

Vast amounts of information were going to be collected and analyzed, and the available [database](#) technology at the time was insufficient for storing and organizing

such enormous quantities of data. So they developed techniques for virtual data aggregation in order to support effective analysis across heterogeneous databases, as well as unstructured public data sources, such as the World Wide Web. "Effective analysis across heterogeneous databases" means the ability to take things from databases which are designed to store different types of data—such as a database containing criminal records, a [phone call database](#) and a foreign intelligence database. The World Wide Web is considered an "unstructured public data source" because it is publicly accessible and contains many different types of data—such as



blogs, emails, records of visits to web sites, etc.—all of which need to be analyzed and stored efficiently.^[21]

Another goal was to develop "a large, distributed system architecture for managing the huge volume of raw data input, analysis results, and feedback, that will result in a simpler, more flexible data store that performs well and allows us to retain important data indefinitely."^[21]

Genisys had an internal "Privacy Protection Program." It was intended to restrict analysts' access to irrelevant information on private U.S. citizens, enforce [privacy laws](#) and policies via software mechanisms, and report misuse of data.^[22]

Scalable Social Network Analysis [[edit](#)]

Scalable Social Network Analysis (SSNA) aimed at developing techniques based on [social network analysis](#) for modeling the key characteristics of terrorist groups and discriminating these groups from other types of societal groups.^[23]

Sean McGahan, of [Northeastern University](#) said the following in his study of SSNA:

The purpose of the SSNA algorithms program is to extend techniques of social network analysis to assist with distinguishing potential terrorist cells from legitimate groups of people ... In order to be successful SSNA will require information on the social interactions of the majority of people around the globe. Since the Defense Department cannot easily distinguish between peaceful citizens and terrorists, it will be necessary for them to gather data on innocent civilians as well as on potential terrorists.

— Sean McGahan^[23]

Futures Markets Applied to Prediction (FutureMAP) [[edit](#)]

Main article: [Future Map](#)

Further information: [Policy Analysis Market](#)

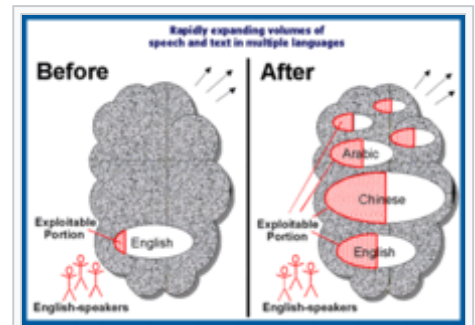
Futures Markets Applied to Prediction (FutureMAP) was intended to harness [collective intelligence](#) by researching [prediction market](#) techniques for avoiding surprise and predicting future events. The intent was to explore the feasibility of market-based trading mechanisms to predict political instability, threats to national security, and other major events in the near future.^[24] In laymans terms, FutureMap would be a website that allowed people to bet on when a terrorist attack would occur.^[25] The bookie would have been the federal government.^[25] Several Senators were outraged at the very notion of such a program.^[25] Then Senate Minority Leader Tom Daschle said on the floor of the Senate "I couldn't believe that we would actually commit \$8 million to create a Web site that would encourage investors to bet on futures involving terrorist attacks and public assassinations. ... I can't believe that anybody would seriously propose that we trade in death. ... How long would it be before you saw traders investing in a way that would bring about the desired result?"^[25] Democratic Senator from Oregon, Ron Wyden said, "The idea of a federal betting parlor on atrocities and terrorism is ridiculous and it's grotesque."^[25] The ranking Democrat on the Armed Services Committee, Sen. Carl Levin of

Michigan, thought the program was so ridiculous that he thought initial reports of it were the result of a hoax.^[25] The program was then dropped.

TIDES [\[edit \]](#)

Translingual Information Detection, Extraction and Summarization (TIDES) developing advanced language processing technology to enable English speakers to find and interpret critical information in multiple languages without requiring knowledge of those languages.^[26]

Outside groups (such as universities, corporations, etc.) were invited to participate in the annual [information retrieval](#), topic detection and tracking, automatic content extraction, and [machine translation](#) evaluations run by [NIST](#).^[26]



Goals of the Translingual Information Detection, Extraction and Summarization (TIDES) project

Genoa / Genoa II [\[edit \]](#)

Genoa and **Genoa II** focused on providing advanced decision-support and collaboration tools to rapidly deal with and adjust to dynamic crisis management and allow for inter-agency collaboration in real-time.^{[27][28]} Another function was to be able to make estimates of possible future scenarios to assist intelligence officials in deciding what to do,^[29] in a manner similar to the DARPA's [Deep Green](#) program which is designed to assist Army commanders in making battlefield decisions.

Wargaming the Asymmetric Environment (WAE) [\[edit \]](#)

Wargaming the Asymmetric Environment (WAE) focused on developing automated technology capable of identifying predictive indicators of terrorist activity or impending attacks by examining individual and group behavior in broad environmental context and examining the motivation of specific terrorists.^[30]

Effective Affordable Reusable Speech-to-text (EARS) [\[edit \]](#)

Effective Affordable Reusable Speech-to-text (EARS) to develop automatic [speech-to-text](#) transcription technology whose output is substantially richer and much more accurate than previously possible. EARS was to focus on everyday human-to-human speech from broadcasts and telephone conversations in multiple languages.^[31] It is expected to increase the speed with which speech can be processed by computers by 100 times or more.^[29]



Graphic from the Information Awareness Office's website describing the goals of the Effective, Affordable, Reusable Speech-to-Text (EARS) project

The intent is to create a core enabling technology (technology that is used as a component for future technologies) suitable for a wide range of future surveillance

applications.^[31]

Babylon [[edit](#)]

Babylon to develop rapid, two-way, natural language speech translation interfaces and platforms for the warfighter for use in field environments for force protection, refugee processing, and medical triage.^[32]

Bio-Surveillance [[edit](#)]

Bio-Surveillance to develop the necessary information technologies and resulting prototype capable of detecting the covert release of a biological pathogen automatically, and significantly earlier than traditional approaches.^[33]

Communicator [[edit](#)]

Communicator was to develop "dialogue interaction" technology that enables warfighters to talk with computers, such that information will be accessible on the battlefield or in command centers without ever having to touch a keyboard.

The Communicator Platform

was to be both wireless and mobile, and to be designed to function in a networked environment.^[34]

The dialogue interaction software was to interpret the *context* of the dialogue in order to improve performance, and to be capable of automatically adapting to new topics (because situations quickly change in war) so conversation is natural and efficient. The Communicator program emphasized task knowledge to compensate for natural language effects and noisy environments. Unlike automated translation of [natural language](#) speech, which is much more complex due to an essentially unlimited vocabulary and grammar, the Communicator program is directed task specific issues so that there are constrained vocabularies (the system only needs to be able to understand language related to war). Research was also started to focus on foreign language computer interaction for use in supporting coalition operations.^[34]

Live exercises were conducted involving small unit logistics operations involving the [United States Marines](#) to test the technology in extreme environments.^[34]

Components of TIA projects that continue to be developed [[edit](#)]

Despite the withdrawal of funding for the TIA and the closing of the IAO, the core of the project survived.^{[11][12][35]} Legislators included a classified annex to the Defense Appropriations Act that preserved funding for TIA's component technologies, if they were transferred to other government agencies. TIA projects continued to be funded



Diagram (from official IAO site) describing capabilities of the "Communicator" project

under classified annexes to Defense and Intelligence appropriation bills. However, the act also stipulated that the technologies only be used for military or foreign intelligence purposes against foreigners.^[36]

TIA's two core projects are now operated by Advanced Research and Development Activity (ARDA) located among the 60-odd buildings of "Crypto City" at NSA headquarters in Fort Meade, MD. ARDA itself has been shifted from the NSA to the [Disruptive Technology Office](#) (run by the [Director of National Intelligence](#)). They are funded by National Foreign Intelligence Program for foreign counterterrorism intelligence purposes.

One technology, codenamed "Basketball" is the Information Awareness Prototype System, the core architecture to integrate all the TIA's information extraction, analysis, and dissemination tools. Work on this project is conducted by [SAIC](#) through its former [Hicks & Associates](#) consulting arm run by former Defense and military officials and which had originally been awarded US\$19 million IAO contract to build the prototype system in late 2002.^[37]

The other project has been re-designated "Topsail" (formerly [Genoa II](#)) and would provide IT tools to help anticipate and preempt terrorist attacks. SAIC has also been contracted to work on Topsail, including a US\$3.7 million contract in 2005.

Media coverage and criticism [edit]

The first mention of the IAO in the mainstream media came from *The New York Times* reporter [John Markoff](#) on February 13, 2002.^[38] Initial reports contained few details about the program. In the following months, as more information emerged about the scope of the TIA project, [civil libertarians](#) became concerned over what they saw as the potential for the development of an [Orwellian](#) mass surveillance system.


On November 14, 2002, *The New York Times* published a column by [William Safire](#) in which he claimed "[TIA] has been given a \$200 million budget to create computer dossiers on 300 million Americans."^[39] Safire has been credited with triggering the anti-TIA movement.^[40]

See also [edit]

- [ADVISE](#), full population data mining & analysis to "monitor social threats"
- [Carnivore](#), FBI US digital interception program
- [Combat Zones That See](#), or CTS, a project to link up all security cameras citywide and "track everything that moves".
- [Communications Assistance For Law Enforcement Act](#)
- [ECHELON](#), NSA worldwide digital interception program
- [Fusion center](#)
- [Government Information Awareness](#)
- [Information Processing Technology Office](#)
- [Intellipedia](#), a collection of wikis used by the U.S. intelligence community to "connect the dots" between pieces of intelligence
- [MALINTENT](#)—similar program to HumanID

- [Mass surveillance](#)
- [Multistate Anti-Terrorism Information Exchange](#)
- [Pre-crime](#) concept in criminology
- [PRISM \(surveillance program\)](#)
- [Synthetic Environment for Analysis and Simulations](#)
- [TALON \(database\)](#)
- [Utah Data Center](#)

References [[edit](#)]

- [^] ["Information Awareness Office"](#) ↗. DARPA. Archived from [the original](#) ↗ on 2 August 2002.
- [^] Tim Dowling. ["What does the Prism logo mean?"](#) ↗. *The Guardian*. Retrieved 30 November 2013. "The Prism logo is slightly more opaque than the one used by the US government's Information Awareness Office, which boasted an all-seeing eye atop a pyramid, casting a golden light across an adjacent planet Earth."
- [^] Hendrik Hertzberg (December 9, 2002). ["Too Much Information"](#) ↗. *The New Yorker*. Retrieved 30 November 2013. "The Information Awareness Office's official seal features an occult pyramid topped with mystic all-seeing eye, like the one on the dollar bill. Its official motto is "Scientia Est Potentia," which doesn't mean "science has a lot of potential." It means "knowledge is power.""
- [^] Jonathan Turley (November 17, 2002). ["George Bush's Big Brother"](#) ↗. *The Los Angeles Times*. Retrieved 19 December 2013.
- [^] [a](#) [b](#) James Poulos. ["Obama Administration Anti-Leak Scheme Shows Precrime and Total Information Awareness Go Hand In Hand"](#) ↗. *Forbes*. Retrieved 19 October 2013.
- [^] [a](#) [b](#) John Horgan. ["U.S. Never Really Ended Creepy "Total Information Awareness" Program"](#) ↗. *Scientific American*. Retrieved 19 October 2013.
- [^] John Markoff (November 22, 2002). ["Pentagon Plans a Computer System That Would Peek at Personal Data of Americans"](#) ↗. *The New York Times*.
- [^] [a](#) [b](#) [c](#) [Total Information Awareness \(TIA\)](#) ↗, *Electronic Privacy Information Center (EPIC)*
- [^] [Dismantling the Empire: America's Last Best Hope](#) By Chalmers Johnson ISBN 0-8050-9303-6 "Congress's action did not end the Total Information Awareness program. The National Security Agency secretly decided to continue it through its private contractors."
- [^] ["Total/Terrorism Information Awareness \(TIA\): Is It Truly Dead?"](#) ↗. *Electronic Frontier Foundation (official website)*. 2003. Archived from [the original](#) ↗ on 2009-03-25. Retrieved 2009-03-15.
- [^] [a](#) [b](#) [c](#) Harris, Shane (Feb 23, 2006). ["TIA Lives On"](#) ↗. *National Journal*. Archived from [the original](#) ↗ on May 28, 2011. Retrieved 2009-03-16.
- [^] [a](#) [b](#) [c](#) ["U.S. Still Mining Terror Data"](#) ↗. *Wired News*. February 23, 2004.
- [^] [a](#) [b](#) [c](#) Lundin, Leigh (7 July 2013). ["Pam, Prism, and Poindexter"](#) ↗. *Spying*. Washington: SleuthSayers. Retrieved 4 January 2014.
- [^] [Overview of the Information Awareness Office](#) ↗
- [^] [Search Results - THOMAS \(Library of Congress\)](#) ↗
- [^] [The Global Information Society Project](#) ↗ 
- [^] Department of Defense Appropriations Act, 2004, Pub. L. No. 108–87, § 8131, 117 Stat. 1054, 1102 (2003)
- [^] 149 Cong. Rec. H8755—H8771 (24 September 2003)

19. ^{^ a b c} "Human Identification at a distance" [↗](#). *Information Awareness Office (official website -- mirror)*. Archived from [the original](#) [↗](#) on February 15, 2009. Retrieved 2009-03-15.
20. ^{^ a b c} "Evidence Extraction and Link Discovery" [↗](#). *Information Awareness Office (official website -- mirror)*. Archived from [the original](#) [↗](#) on 2009-02-15. Retrieved 2009-03-15.
21. ^{^ a b c} "Genisys" [↗](#). *Information Awareness Office (official website)*. Archived from [the original](#) [↗](#) on 2009-02-16. Retrieved 2009-03-15.
22. [^] Lee, Newton (7 April 2015). *Counterterrorism and Cybersecurity: Total Information Awareness* [↗](#) (2, illustrated, revised ed.). Springer. p. 141. ISBN 9783319172446.
23. ^{^ a b} Ethier, Jason. "Current Research in Social Network Theory" [↗](#). *Northeastern University College of Computer and Information Science*. Archived from [the original](#) [↗](#) on February 26, 2015. Retrieved 2009-03-15.
24. [^] FutureMap [↗](#) Archived [↗](#) 2006-02-05 at the [Wayback Machine](#)
25. ^{^ a b c d e f} CNN [↗](#)
26. ^{^ a b} "TIDES" [↗](#). *Information Awareness Office (official website -- mirror)*. Archived from [the original](#) [↗](#) on 2009-02-15. Retrieved 2009-03-15.
27. [^] "Genoa" [↗](#). *Information Awareness Office (official website)*. Archived from [the original](#) [↗](#) on 2009-02-16. Retrieved 2009-03-15.
28. [^] "Genoa II" [↗](#). *Information Awareness Office (official website)*. Archived from [the original](#) [↗](#) on 2009-02-15. Retrieved 2009-03-15.
29. ^{^ a b} Belasco, Amy (January 21, 2003). "EFF: Memorandum Regarding TIA Funding" [↗](#). *Electronic Frontier Foundation*. Retrieved 2009-03-15.
30. [^] "Wargaming the Asymmetric Environment (WAE)" [↗](#). *www.darpa.mil/iao*. Information Awareness Office. Archived from [the original](#) [↗](#) on 28 May 2012. Retrieved 16 June 2016.
31. ^{^ a b} "EARS" [↗](#). *Information Awareness Office (official website -- mirror)*. Retrieved 2009-03-15.
32. [^] Babylon [↗](#) Archived [↗](#) 2006-07-15 at the [Wayback Machine](#)
33. [^] BSS [↗](#) Archived [↗](#) 2006-09-19 at the [Wayback Machine](#)
34. ^{^ a b c} "Communicator" [↗](#). *Information Awareness Office (official website)*. Archived from [the original](#) [↗](#) on 2009-02-15. Retrieved 2009-03-15.
35. [^] Wanted: Competent Big Brothers [↗](#) Archived [↗](#) 2008-05-17 at the [Wayback Machine](#), *Newsweek*, 8 February 2006, retrieved 27 July 2007
36. [^] The Total Information Awareness Project Lives On [↗](#), *Technology Review*, 26 April 2006, retrieved 27 July 2007
37. [^] TIA Lives On [↗](#), *National Journal*, 23 February 2006, retrieved 27 July 2007
38. [^] Markoff, John (February 13, 2002). "Chief Takes Over at Agency To Thwart Attacks on U.S." [↗](#). *The New York Times*. Retrieved May 5, 2010.
39. [^] Safire, William (2002-11-14). "You Are a Suspect" [↗](#). *The New York Times*. p. 2. Retrieved 2010-10-21.
40. [^] Big Brother ... [↗](#)

Further reading [\[edit \]](#)

- Copies of the original IAO web pages formerly available at <https://web.archive.org/web/20021123234437/http://www.darpa.mil/iao/> [↗](#) (June 12, 2002 – June 3, 2003) can be found at [Archive index](#) [↗](#) at the [Wayback Machine](#)

- John Poindexter, [Overview of the Information Awareness Office](#) (Remarks as prepared for delivery by Dr. John Poindexter, Director, Information Awareness Office, at the DARPA Tech 2002 Conference) (August 2, 2002).

External links [edit]

- [Information Awareness Office](#)

Media coverage [edit]

- Harris, Shane (February 26, 2006). ["TIA Lives On"](#). *The National Journal*. Archived from [the original](#) on May 17, 2008.
- "Pentagon Defends Surveillance Program". *The Washington Post*. May 20, 2003.
- Webb, Cynthia L. (May 21, 2003). "The Pentagon's PR Play". *The Washington Post*.
- Bray, Hiawatha (April 4, 2003). "Mining Data to Fight Terror Stirs Privacy Fears". *The Boston Globe*. pp. C2.
- McCullagh, Declan (January 15, 2003). ["Pentagon database plan hits snag on Hill"](#). CNET News.com.
- Markoff, John (February 13, 2002). ["Chief Takes Over at Agency To Thwart Attacks on U.S."](#) *The New York Times*. pp. (first mainstream media mention of IAO).

Academic articles [edit]

- K. A. Taipale (2003). "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data". *Columbia Sci. & Tech. Law Review*. **5** (2): 1–83 (TIA discussed 39–50). [SSRN 546782](#).
- Robert Popp and John Poindexter (November–December 2006). ["Countering Terrorism through Information and Privacy Protection Technologies"](#) (PDF). *IEEE Security & Privacy*: 18–26.




Critical views [edit]

- ["TIA: Total Information Awareness"](#). American Civil Liberties Union. January 16, 2004.
- Charles V. Peña (November 22, 2002). ["TIA: Information Awareness Office Makes Us a Nation of Suspects"](#). Cato Institute. Archived from [the original](#) on December 1, 2002.
- ["Total/Terrorism Information Awareness \(TIA\): Is It Truly Dead? EFF: It's Too Early to Tell"](#). Electronic Frontier Foundation.
- ["Total "Terrorism" Information Awareness \(TIA\): Latest News"](#). Electronic Privacy Information Center.
- ["A Times Editorial: Unfocused data-mining"](#). *St. Petersburg Times*. January 24, 2003.
- Russ Kick. ["Information Awareness Office Website Deletes Its Logo"](#). The Memory Hole.

Proponent views [edit]

- Mac Donald, Heather (January 27, 2003). "Total Misrepresentation" [↗](#). *The Weekly Standard*.
- Levin, Jonathan (February 13, 2003). "Total Preparedness: The case for the Defense Department's Total Information Awareness project" [↗](#). *National Review*.
- Taylor, Jr., Stuart (December 10, 2002). "Big Brother and Another Overblown Privacy Scare" [↗](#). *The Atlantic*. Archived from the original [↗](#) on December 26, 2002.

Accord:

- Shane Ham & Robert D. Atkinson (2002). "Using Technology to Detect and Prevent Terrorism"  (PDF). Progressive Policy Institute. Archived from the original  (PDF) on 2007-09-26.
- "Safeguarding Privacy in the Fight Against Terrorism"  (PDF). DOD Technology and Privacy Advisory Committee (TAPAC). March 2004.

Also:

- Ignatius, David (August 1, 2003). "Back in the Safe Zone" [↗](#). *The Washington Post*. pp. A19 (discussing opposition to the IAO FutureMap project).

Categories: [DARPA offices](#) | [Government databases in the United States](#)
| [Mass surveillance](#) | [2002 establishments in the United States](#)
| [Organizations established in 2002](#)

This page was last edited on 22 September 2019, at 16:46 (UTC).

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.

[Privacy policy](#) [About Wikipedia](#) [Disclaimers](#) [Contact Wikipedia](#) [Developers](#) [Cookie statement](#)

[Mobile view](#)

