Safeguarding Privacy in the Fight Against Terrorism

REPORT OF THE TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE

Executive Summary

March 2004

SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM

The Report of the Technology and Privacy Advisory Committee

Executive Summary

MARCH 2004

DEPARTMENT OF DEFENSE
TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE
3330 Defense Pentagon, Room 3E1045
Washington, DC 20301-3330

March 1, 2004

The Hon. Donald H. Rumsfeld
Secretary of Defense
Department of Defense
1000 Defense Pentagon 3E880
Washington, DC 20301-1000

Dear Secretary Rumsfeld:

In February 2003, you appointed the Technology and Privacy Advisory Committee to examine the Terrorism Information Awareness program and to develop safeguards "to ensure that the application of this or any like technology developed within DOD is carried out in accordance with U.S. law and American values related to privacy." We are pleased to provide you with our final report.

TIA was only one of the programs within DOD and elsewhere in the government involved, or with the potential for being involved, in data mining concerning U.S. persons. The committee believes that data mining plays a critical role in the fight against terrorism, but that it should be used—and can be effectively—only in ways that do not compromise the privacy of U.S. persons. That is the goal of our recommendations. We believe our recommendations both protect privacy and facilitate the appropriate, effective, and efficient use of data mining tools to fight terrorism.

While we have focused on DOD, we do not believe that all of the necessary safeguards are within the power of the Secretary of Defense. Some of our recommendations therefore encourage you to recommend to the President and Congress actions we believe are necessary to ensure meaningful privacy protection not only in DOD, but throughout the government. These recommendations are designed to create a consistent, government-wide standard to facilitate the sharing of information among agencies that is critical to fighting terrorism.

The committee's deliberations have been substantive, wide-ranging, and collegial. The committee is unanimous in most of its recommendations. A separate statement from William T. Coleman, Jr., reflecting his opposition to some of the committee's conclusions, is appended to our report. A separate statement from Floyd Abrams, which highlights why the committee disagrees with many of the views expressed in Mr. Coleman's statement, is also appended. Those statements and the seriousness of our discussions reflect the importance and difficulty of these issues.

The committee's work was greatly aided by the testimony of 60 witnesses from DOD, other government agencies, private industry, academia, and advocacy groups, and by extensive briefings for individual committee members and staff from many other individuals. These people are acknowledged individually in our report, but we wish to take this opportunity to thank them once again for their dedicated and selfless public service. Finally, I express my gratitude for the commitment, cooperation, and tireless work of the committee members; Lisa Davis, the committee's Executive Director and Designated Federal Official; and Professor Fred H. Cate, the committee's Reporter.

Yours sincerely,

Newton N. Minow

Newton N. Minow
Chairman

TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE

Newton N. Minow
Chairman

Floyd Abrams
Zoë Baird
Griffin Bell
Gerhard Casper
William T. Coleman, Jr.
Lloyd N. Cutler
John O. Marsh, Jr.

Lisa A. Davis
Executive Director and Designated Federal Official

Fred H. Cate
Reporter

The document contains the executive summary and other selected material from TAPAC's final report. The complete report is available online on the committee's website at *www.sainc.com/TAPAC*.

Contents

List of Abbreviations and Defined Terms

ARDA	Advanced Research and Development Activity
"General Crimes Guidelines"	Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations
CAPPS II	Second generation Computer-Assisted Passenger Prescreening System, a TSA project
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
"Data Mining"	Searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government
DHS	Department of Homeland Security
DOD	Department of Defense
ECPA	Electronic Communications Privacy Act
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FTC	Federal Trade Commission
GAO	General Accounting Office
IAO	Information Awareness Office, a former DARPA office
INS	Immigration and Naturalization Service
IT	Information technology
MATRIX	Multistate Anti-Terrorism Information Exchange
OECD	Organization for Economic Cooperation and Development
"OECD Guidelines"	Guidelines on the Protection of Privacy and Transborder Flows of Personal Data issued by the OECD Committee of Ministers in 1974
OMB	Office of Management and Budget
SSNs	Social Security Numbers
TALON	Threat Alerts and Locally Observed Notices
TAPAC	Technology and Privacy Advisory Committee
TIA	Terrorism (formerly "Total") Information Awareness, a former DARPA project
TSA	Transportation Security Administration
"U.S. person"	Defined by Executive Order 12333 as an individual who is a U.S. citizen or permanent resident alien, a group or organization that is an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation incorporated in the United States (except if directed and controlled by a foreign government or governments). Because TAPAC is concerned only with the privacy interests of individuals, the report uses the term to refer only to a U.S. citizen or permanent resident alien.
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

Executive Summary

[Terrorism] poses extraordinary risks to our security, as well as to our constitutional freedoms, which could all too easily be compromised in the fight against this new and deadly terrorist threat.

TAPAC's Creation and Charge

The United States faces, in the words of British Prime Minister Tony Blair, "a new and deadly virus."[1] That virus is "terrorism, whose intent to inflict destruction is unconstrained by human feeling and whose capacity to inflict it is enlarged by technology."[2]

As the murderous attacks of September 11 painfully demonstrated, this new threat is unlike anything the nation has faced before. The combination of coordinated, well-financed terrorists, willing to sacrifice their lives, potentially armed with weapons of mass destruction, capable of operating within our own borders poses extraordinary risks to our security, as well as to our constitutional freedoms, which could all too easily be compromised in the fight against this new and deadly terrorist threat. To help guard against this, Secretary of Defense Donald Rumsfeld appointed the Technology and Privacy Advisory Committee ("TAPAC") in February 2003 to examine the use of "advanced information technologies to identify terrorists before they act."[3]

Secretary Rumsfeld charged the committee with developing safeguards "to ensure that the application of this or any like technology developed within [the Department of Defense] DOD is carried out in accordance with U.S. law and American values related to privacy."[4]*

The decision to create TAPAC was prompted by the escalating debate over the Terrorism Information Awareness ("TIA") program.† TIA had

* U.S. laws apply to surveillance, searches, and seizures of personally identifiable information conducted or authorized by government officials within the United States. Those laws apply outside of the United States only if the surveillance, search, or seizure involves a U.S. citizen (although not necessarily a permanent resident alien).

This report focuses exclusively on the privacy issues posed by U.S. government data mining programs under U.S. law to U.S. persons, which are defined under U.S. law as U.S. citizens and permanent resident aliens. It does not address data mining concerning federal government employees in connection with their employment.

† When first announced, the program was entitled "Total Information Awareness." The title was changed to "Terrorism Information Awareness" in May 2003.

TIA was not unique in its potential for data mining. . . . [M]any other programs in use or under development . . . make similar uses of personal information concerning U.S. persons to detect and deter terrorist activities.

been created by the Defense Advanced Research Projects Agency ("DARPA") in 2002 as a tool to "become much more efficient and more clever in the ways we find new sources of data, mine information from the new and old, generate information, make it available for analysis, convert it to knowledge, and create actionable options."[5]

TIA sparked controversy in Congress and the press, due in large part to the threat it was perceived as posing to informational privacy. On September 25, 2003, Congress terminated funding for the program with the exception of "processing, analysis, and collaboration tools for counter-terrorism foreign intelligence," specified in a classified annex to the Act. These tools may be used only in connection with "lawful military operations of the United States conducted outside the United States" or "lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States citizens."[6] This language makes clear that TIA-like activities may be continuing.

The Scope of Government Data Mining

TIA was not unique in its potential for data mining.* TAPAC is aware of many other programs in use or under development both within DOD and elsewhere in the government that make similar uses of personal information concerning U.S. persons to detect and deter terrorist activities, including:

- DOD programs to determine whether data mining can be used to identify individuals who pose a threat to U.S. forces abroad
- the intelligence community's Advanced Research and Development Activity center, based in the National Security Agency, to conduct "advanced research and development related to extracting intelligence from, and providing security for, information transmitted or manipulated by electronic means"[7]
- the Computer-Assisted Passenger Prescreening System in the Department of Homeland Security ("DHS")
- the Treasury Department's Financial Crimes Enforcement Network
- federally mandated "Know Your Customer" rules
- the "MATRIX" (Multistate Anti-Terrorism Information Exchange) system to link law enforcement records with other government and private-sector databases in eight states and DHS
- Congress' mandate in the Homeland Security Act that DHS "establish and utilize . . . a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools," to "access, receive, and analyze data detect and identify threats of terrorism against the United States"[8]

TAPAC's Conclusions

After many public hearings, numerous background briefings, and extensive research, TAPAC has reached four broad conclusions:

TIA was a flawed effort to achieve worthwhile ends. It was flawed by its perceived insensitivity to

* We define "data mining" to mean: searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government.

TIA was a flawed effort to achieve worthwhile ends. It was flawed by its perceived insensitivity to critical privacy issues, the manner in which it was presented to the public, and the lack of clarity and consistency with which it was described.

critical privacy issues, the manner in which it was presented to the public, and the lack of clarity and consistency with which it was described. DARPA stumbled badly in its handling of TIA, for which the agency has paid a significant price in terms of its credibility in Congress and with the public. This comes at a time when DARPA's historically creative and ambitious research capacity is more necessary than ever. By maintaining its focus on imaginative, far-sighted research, at the same time that it takes account of informational privacy concerns, DARPA should rapidly regain its bearings. It is in the best interests of the nation for it to do so.

Data mining is a vital tool in the fight against terrorism, but when used in connection with personal data concerning U.S. persons, data mining can present significant privacy issues. Data mining tools, like most technologies, are inherently neutral: they can be used for good or ill. However, when those tools are used by the government to scrutinize personally identifiable data concerning U.S. persons who have done nothing to warrant suspicion, if they are conducted without an adequate predicate they run the risk of becoming the 21st-century equivalent of general searches, which the authors of the Bill of Rights were so concerned to protect against.

To be certain, data mining has many valuable and lawful uses in both the private and public sectors. In many settings it may prove less intrusive to privacy than other techniques for guarding against terrorist threats. Moreover, the same technologies that make data mining feasible can be used to reduce the amount of personally identifiable data necessary, facilitate data mining with anonymized data, and create immutable audit trails and other protections against misuse.

However, when data mining involves the government accessing personally identifiable information about U.S. persons, it also raises privacy issues. The magnitude of those issues varies depending upon many factors, including: the sensitivity of the data being mined, the expectation of privacy reasonably associated with the data, the consequences of an individual being identified by an inquiry, and the number (or percentage) of U.S. persons identified in response to an inquiry who have not otherwise done anything to warrant government suspicion.

In developing and using data mining tools the government can and must protect privacy. This has never been more starkly presented than following the September 11 terrorist attacks, which vividly demonstrated the need to deploy the tools

Data mining is a vital tool in the fight against terrorism, but when used in connection with personal data concerning U.S. persons, data mining can present significant privacy issues.

necessary to protect and defend the nation without violating our constitutional values in the process.

Striking a balance between security and privacy is no easy task. Alexander Hamilton wrote in Federalist Paper 8 in 1787 that "[s]afety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates." "To be more safe," he concluded, nations "at length become willing to run the risk of being less free."[9] The Supreme Court wrote in 1963 that it is "under the pressing exigencies of crisis, that there is the greatest temptation to dispense with fundamental constitutional guarantees which, it is feared, will inhibit governmental action."[10]

This is precisely the challenge our nation faces today, a challenge made immediate and critical by the magnitude of the terrorist threat, its sustained nature, and the fact that it comes not from an identified enemy abroad but from a largely invisible enemy that may be operating within our borders.

Existing legal requirements applicable to the government's many data mining programs are numerous, but disjointed and often outdated, and as a result may compromise the protection

Data Mining Checklist

The Existence and Purpose of Data Mining

1. Is the proposed activity or system likely to involve the acquisition, use, or sharing of personally identifiable information about U.S. persons?
2. What purpose(s) does the data mining serve? Is it lawful? Is it within the agency's authority? Is it sufficiently important to warrant the risks to informational privacy that data mining poses?
3. Is data mining necessary to accomplish that purpose—i.e., could the purpose be accomplished as well without data mining?
4. Is the data mining tool designed to access, use, retain, and disseminate the least data necessary to serve the purposes for which it is intended?
5. Is the data mining tool designed to use anonymized data whenever possible?

Data Mining Personally Identifiable Information

6. Are there specific and articulable facts that data mining personally identifiable information (or reidentifying previously anonymized information) concerning U.S. persons will be conducted in a manner that otherwise complies with the requirements of applicable laws and recommendations; is reasonably related to identifying or apprehending terrorists, preventing terrorist attacks, or locating or preventing the use of weapons of mass destruction; is likely to yield information relevant to national security; and is not practicable with anonymized data?

The Sources and Nature of Data Concerning U.S. Persons

7. Are the data appropriate for their intended use, taking into account the purpose(s) for which the data were collected, their age, and the conditions under which they have been stored and protected?
8. Are data being accessed or acquired from third parties in violation of the terms and conditions (usually reflected in a privacy policy) under which they were collected?
9. If data are being acquired directly from data subjects, have the individuals been provided with appropriate notice, consistent with the purpose of the data mining activity?

Existing legal requirements applicable to the government's many data mining programs . . . may compromise the protection of privacy, public confidence, and the nation's ability to craft effective and lawful responses to terrorism.

of privacy, public confidence, and the nation's ability to craft effective and lawful responses to terrorism. This is especially true in the setting on which TAPAC focused—analyzing personally identifiable data to protect against terrorist threats.

The legal protections that have historically applied in this context recognize distinctions between U.S. persons and non-U.S. persons, and between law enforcement and national security, and between activities that take place in the United States as

10 Are data being sought in the order provided by Executive Order 12333—i.e., from or with the consent of the data subject, from publicly available sources, from proprietary sources, through a method requiring authorization less than probable cause (e.g., a pen register or trap and trace device), through a method requiring a warrant, and finally through a method requiring a wiretap order?

11 Are personally identifiable data being left in place whenever possible? If such data are being acquired or transferred, is there a system in place for ensuring that they are returned or destroyed as soon as practicable?

The Impact of Data Mining

12 What are the likely effect(s) on individuals identified through the data mining—i.e., will they be the subject of further investigation or will they be immediately subject to some adverse action?

13 Does the data mining tool yield a rate of false positives that is acceptable in view of the purpose of the search, the severity of the effect of being identified, and the likelihood of further investigation?

14 Is there an appropriate system in place for dealing with false positives (e.g., reporting false positives to developers to improve the system, correcting incorrect information if possible, etc.), including identifying the frequency and effects of false positives?

Oversight of Data Mining

15 Are data secured against accidental or deliberate unauthorized access, use, alteration, or destruction, and access to the data mining tool restricted to persons with a legitimate need and protected by appropriate access controls taking into account the sensitivity of the data?

16 Does the data mining tool generate, to the extent technologically possible, an immutable audit trail showing which data have been accessed or transferred, by what users, and for what purposes?

17 Will the data mining tool be subject to continual oversight to ensure that it is used appropriately and lawfully, and that informational privacy issues raised by new developments or discoveries are identified and addressed promptly?

18 Are all persons engaged in developing or using data mining tools trained in their appropriate use and the laws and regulations applicable to their use?

19 Have determinations as to the efficacy and appropriateness of data mining been made or reviewed by an official other than those intimately involved with the development, acquisition, or use of the data mining tool?

Clear, uniform laws and standards governing data mining are necessary . . . to use data mining tools effectively and aggressively in the fight against terrorism.

opposed to those that take place beyond our borders. This "line at the border" approach to privacy law and to national security is now increasingly inadequate because of the new threat from terrorists who may be operating within our borders, and advances in digital technologies, including the Internet, that have exponentially increased the volume of data available about individuals and greatly reduced the financial and other obstacles to retaining, sharing, and transferring those data across borders. These developments highlight the need for new regulatory boundaries to help protect civil liberties and national security at the same time. It is time to update the law to respond to new challenges.

The stakes could not be higher. Clear, uniform laws and standards governing data mining are necessary to empower DOD and other government agencies to use data mining tools effectively and aggressively in the fight against terrorism. Those laws and standards are also necessary to protect informational privacy, which is both important in its own right and is often critical to a range of fundamental civil liberties, including our rights to speak, protest, associate, worship, and participate in the political process free from government intrusion or intimidation.

Recommendations Concerning DOD Data Mining

We believe it is possible to use information technologies to protect national security without compromising the privacy of U.S. persons. The answer lies in clear rules and policy guidance, adopted through an open and credible political process, supplemented with educational and technological tools, developed as an integral part of the technologies that threaten privacy, and enforced through appropriate managerial, political, and judicial oversight.

Recommendation 1

DOD should safeguard the privacy of U.S. persons when using data mining to fight terrorism.

Recommendation 2

The Secretary should establish a regulatory framework applicable to all data mining conducted by, or under the authority of, DOD, known or reasonably likely to involve personally identifiable information concerning U.S. persons. The essential elements of that framework include a written finding by agency heads authorizing data mining; minimum technical requirements for data mining systems (including data minimization, data anonymization, creation of an audit trail, security and access controls, and training for personnel involved in data mining); special protections for data mining involving databases from other government agencies or from private industry; authorization from the Foreign Intelligence Surveillance Court before engaging in data mining with personally identifiable information concerning U.S. persons or reidentifying previously anonymized information concerning U.S. persons; and regular audits to ensure compliance.

We recommend *excluding* from these requirements data mining that is limited to foreign intelligence that does not involve U.S. persons; data mining concerning federal government employees in connection with their employment; and data mining that is based on particularized suspicion, including searches to identify or locate a specific individual (e.g., a suspected terrorist) from airline or cruise ship passenger manifests or other lists of names or other nonsensitive information about U.S. persons.

Summary of TAPAC Recommendations

Recommendations Concerning DOD Data Mining

Recommendation 1

DOD should safeguard the privacy of U.S. persons when using data mining to fight terrorism. "Data mining" is defined to mean: searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government.

Recommendation 2

The Secretary should establish a regulatory framework applicable to all data mining conducted by, or under the authority of, DOD, known or reasonably likely to involve personally identifiable information concerning U.S. persons. The requirements of this section apply to all DOD programs involving data mining concerning U.S. persons, with three exceptions: data mining (1) based on particularized suspicion, including searches of passenger manifests and similar lists; (2) that is limited to foreign intelligence that does not involve U.S. persons; or (3) that concerns federal government employees in connection with their employment. Data mining that is limited to information that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law—should be conditioned only on the written authorization described in Recommendation 2.1 and the compliance audits described in Recommendation 2.5. All other data mining concerning U.S. persons should comply with all of the following requirements:

Recommendation 2.1

Written finding by agency head authorizing data mining. Before an agency can employ data mining known or reasonably likely to involve data concerning U.S. persons, the agency head should first make a written finding that complies with the requirements of this recommendation authorizing the data mining.

An agency head may make the written finding described above either for programs that include data mining as one element, and data mining concerning U.S. persons may occur, or for specific applications of data mining where the use of information known or likely to concern U.S. persons is clearly anticipated.

Recommendation 2.2

Technical requirements for data mining. Data mining of databases known or reasonably likely to include personally identifiable information about U.S. persons should employ or be subject to the requirements of this recommendation (i.e., data minimization, data anonymization, audit trail, security and access, and training).

Recommendation 2.3

Third-party databases. Data mining involving databases from other government agencies or from private industry may present special risks. Such data mining involving, or reasonably likely to involve, U.S. persons, should adhere to the principles set forth in this recommendation.

Recommendation 2.4

Personally identifiable information. It is not always possible to engage in data mining using anonymized data. Moreover, even searches involving anonymized data will ultimately result in matches which must be reidentified using personally identifiable information. The use of personally identifiable information known or reasonably likely to concern U.S. persons in data mining should adhere to the following provisions:

An agency within DOD may engage in data mining using personally identifiable information known or reasonably likely to concern U.S. persons on the condition that, prior to the commencement of the search, DOD obtains from the Foreign Intelligence Surveillance Court a written order authorizing the search based on the existence of specific and articulable facts that meet the requirements of this recommendation.

DOD may seek the approval from the Foreign Intelligence Surveillance Court either for programs that include data mining as one element, and data mining of personally identifiable information known or likely to include information on U.S. persons may arise, or for specific applications of data mining where the use of personally identifiable information known or likely to include information on U.S. persons is clearly anticipated.

An agency may reidentify previously anonymized data known or reasonably likely to concern a U.S. person on the condition that DOD obtains from the Foreign Intelligence Surveillance Court a written order authorizing the reidentification based on the existence of specific and articulable facts that meet the requirements of this recommendation.

Without obtaining a court order, the government may, in exigent circumstances, search personally identifiable information or reidentify anonymized information obtained through data mining if it meets the requirements of this recommendation.

Recommendation 2.5

Auditing for compliance. Any program or activity that involves data mining known or reasonably likely to include personally identifiable information about U.S. persons should be audited not less than annually to ensure compliance with the provisions of this recommendation and other applicable laws and regulations.

Recommendation 3

DOD should, to the extent permitted by law, support research into means for improving the accuracy and effectiveness of data mining systems and technologies, technological and other tools for enhancing privacy protection, and the broader legal, ethical, social, and practical issues in connection with data mining concerning U.S. persons.

Recommendation 4

The Secretary should create a policy-level privacy officer.

Recommendation 5

The Secretary should create a panel of external advisors to advise the Secretary, the privacy officer, and other DOD officials on identifying and resolving informational privacy issues, and on the development and implementation of appropriate privacy protection mechanisms.

Recommendation 6

The Secretary should create and ensure the effective operation of meaningful oversight mechanisms.

Recommendation 7

The Secretary should work to develop a culture of sensitivity to, and knowledge about, privacy issues involving U.S. persons throughout DOD's research, acquisition, and operational activities.

Recommendations Concerning Government Data Mining

Recommendation 8

The Secretary should recommend that Congress and the President establish one framework of legal, technological, training, and oversight mechanisms necessary to guarantee the privacy of U.S. persons in the context of national security and law enforcement activities.

Recommendation 9

The Secretary should recommend that the President appoint an inter-agency committee to help ensure the quality and consistency of federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

Recommendation 10

The Secretary should recommend that the President appoint a panel of external advisors to advise the President concerning federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

Recommendation 11

The Secretary should recommend that the President and Congress take those steps necessary to ensure the protection of U.S. persons' privacy and the efficient and effective oversight of government data mining activities through the judiciary and by this nation's elected leaders through a politically credible process. Specifically, Congress and the President should authorize the Foreign Intelligence Surveillance Court to receive requests for orders under Recommendations 2.4 and 8 and to grant or deny such orders, and each house of Congress should identify a single committee to receive all of the agencies' reports concerning data mining.

Recommendation 12

The Secretary should recommend that the President and Congress support research into means for improving the accuracy and effectiveness of data mining systems and technologies; technological and other tools for enhancing privacy protection; and the broader legal, ethical, social, and practical issues involved with data mining concerning U.S. persons.

In addition, we recommend that data mining that is limited to information that is routinely available without charge or subscription to the public—on the Internet, in telephone directories, or in public records to the extent authorized by law—should be subject to only the requirements that it be conducted pursuant to the written authorization of the agency head (as specified in Recommendation 2.1) and auditing for compliance (as specified in Recommendation 2.5).

Recommendation 3

DOD should, to the extent permitted by law, support research into means for improving the accuracy and effectiveness of data mining systems and technologies, technological and other tools for enhancing privacy protection, and the broader legal, ethical, social, and practical issues in connection with data mining concerning U.S. persons.

Recommendation 4

The Secretary should create a policy-level privacy officer.

Recommendation 5

The Secretary should create a panel of external advisors to advise the Secretary, the privacy officer, and other DOD officials on identifying and resolving informational privacy issues, and on the development and implementation of appropriate privacy protection mechanisms.

Recommendation 6

The Secretary should create and ensure the effective operation of meaningful oversight mechanisms.

Recommendation 7

The Secretary should work to ensure a culture of sensitivity to, and knowledge about, privacy issues involving U.S. persons throughout DOD and all of its research, acquisition, and operational activities. To aid the Secretary in this important task we offer a checklist of questions as a useful guide for identifying specific informational privacy issues related to data mining.

Recommendations Concerning Government Data Mining

While TAPAC focused on TIA and related DARPA programs, it is counterproductive to the protection of both privacy and national security to address only these, while ignoring the many other government programs that use personal information on U.S. persons. Moreover, the privacy issues presented by data mining cannot be resolved by DOD alone. Action by Congress, the President, and the courts is necessary as well. Finally, because DOD is the only federal department to have an external advisory committee to examine the privacy implications of its programs, TAPAC occupies a unique position. We therefore direct our recommendations to the broad range of government data mining activities.

Recommendation 8

The Secretary should recommend that Congress and the President establish one framework of legal, technological, training, and oversight mechanisms necessary to guarantee the privacy of U.S. persons in the context of national security and law enforcement activities. A government-wide approach is desirable to address the significant

While TAPAC focused on TIA and related DARPA programs, it is counterproductive to the protection of both privacy and national security to address only these, . . . ignoring the many other government programs that use personal information.

privacy issues raised by the many programs under development, or already in operation, that involve the use of personally identifiable information concerning U.S. persons for national security and law enforcement purposes.

We therefore believe that the provisions of Recommendation 2, which concern DOD's programs that involve data mining, should also be implemented across the federal government and made applicable to all government departments and agencies that develop, acquire, or use data mining tools in connection with U.S. persons for national security or law enforcement purposes.

We do not suggest that the resolution of informational privacy issues will be the same in every setting. Clearly, some modifications will be necessary. We believe, however, that government efforts to protect national security and fight crime and to protect privacy will be enhanced by the articulation of government-wide principles and a consistent system of laws and processes. National standards will also help provide clear models for state and local government efforts as well.

Recommendation 9

The Secretary should recommend that the President appoint an inter-agency committee to help ensure the quality and consistency of federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

Recommendation 10

The Secretary should recommend that the President appoint a panel of external advisors to advise the President concerning federal government efforts to safeguard informational privacy in the context of national security and law enforcement activities.

Recommendation 11

The Secretary should recommend that the President and Congress take those steps necessary to ensure the protection of U.S. persons' privacy and the efficient and effective oversight of government data mining activities through the judiciary and by this nation's elected leaders through a politically credible process. This includes adopting new, consistent protections, along the lines of these recommendations, for information privacy in the law enforcement and national security contexts. In addition, we believe Congress and the President should work together to enact the legislation necessary to authorize the Foreign Intelligence Surveillance Court to receive requests for orders under Recommendations 2 and 8 and to grant or deny such orders.

There is also a critical need for Congress to exercise appropriate oversight, especially given the fact that many data mining programs may involve classified information which would prevent immediate public disclosure. We believe that each house of Congress should identify a single committee to exercise oversight of data mining activities, and that each agency's privacy officer and agency head should report jointly to those committees at least annually.

Recommendation 12

The Secretary should recommend that the President and Congress support research into means for improving the accuracy and effectiveness of data mining systems and technologies; technological and other tools for enhancing privacy protection; and the broader legal, ethical, social, and practical issues involved with data mining concerning U.S. persons.

Impact of TAPAC Recommendations on Government Data Mining

(i.e., searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government)

Type of Information	New Recommended Requirements
Data mining that is not known or reasonably likely to involve *personally identifiable* information about *U.S. persons* (i.e., U.S. citizens and permanent residents)	No new requirements
Data mining limited to *foreign intelligence* that does not concern *U.S. persons*.	No new requirements
Data mining known or reasonably likely to involve *personally identifiable* information about *U.S. persons*:	
• If based on *particularized suspicion* about a specific individual, including searches to identify or locate a specific individual (e.g., a suspected terrorist) from airline or cruise ship *passenger manifests* or other lists of names or other nonsensitive information about U.S. persons.	No new requirements
• If concerning *federal government employees* that is solely in connection with their employment.	No new requirements
• If limited to searches of information that is *routinely available without charge or subscription to the public*—on the Internet, in telephone directories, or in public records to the extent authorized by law.	1 Administrative authorization (set forth in Recommendation 2.1), which may be granted on a "per program" or "per search" basis; and 2 Regular compliance audits (set forth in Recommendation 2.5).
• If conducted with *deidentified data* (i.e., data from which personally identifying elements such as name or Social Security Number have been removed or obscured)	All new requirements apply (i.e., administrative authorization, compliance with technical requirements, special rules for third-party databases, and regular compliance audits, as set forth in Recommendations 2.1, 2.2, 2.3, and 2.5), *except for* need to obtain a Foreign Intelligence Surveillance Court order (set forth in Recommendation 2.4).
• If conducted with *personally identifiable information.*	All new requirements apply (as set forth in Recommendations 2.1-2.5), *including* application to the Foreign Intelligence Surveillance Court (Recommendation 2.4), which can be made on a "per program" or "per search" basis.

Our goal in these recommendations is to articulate a framework of law and technology to enable the government simultaneously to combat terrorism and safeguard privacy.

Conclusion

Our goal in these recommendations is to articulate a framework of law and technology to enable the government simultaneously to combat terrorism and safeguard privacy. We believe rapid action is necessary to address the host of government programs that involve data mining concerning U.S. persons and to provide clear direction to the people responsible for developing, procuring, implementing, and overseeing those programs.

While these recommendations impose additional burdens on government officials before they employ some data mining tools, we believe that in the long-run they will enhance not only informational privacy, but national security as well. They are designed to help break down the barriers to information-sharing among agencies that have previously hampered national security efforts, to provide sufficient clarity concerning access to and use of personal information concerning U.S. persons so that DOD and other government officials can use such information appropriately, and to ensure that scarce national security resources are deployed strategically and effectively.

This broader, more comprehensive approach is essential if our nation is to achieve its goal of combating terrorism *and* safeguarding the privacy of U.S. persons. We must not sacrifice liberty for security, because as Benjamin Franklin warned more than two centuries ago, "they that can give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety."[11] Franklin might well have added that those who trade liberty for safety all too often achieve neither.

Notes

1 Tony Blair, Address before a Joint Session of Congress, Washington, DC, July 17, 2003.

2 Id.

3 U.S. Department of Defense, Technology and Privacy Advisory Committee Charter (Mar. 25, 2003).

4 Id.

5 John Poindexter, Overview of the Information Awareness Office, prepared remarks for delivery at DARPATech 2002, Anaheim, CA, Aug. 2, 2002, at 1.

6 Department of Defense Appropriations Act, 2004, Pub. L. No. 108-84, § 8183 (Sept. 25, 2003).

7 Memo from CIA Director George Tenet (May 11, 1998).

8 Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 201(d)(1), (d)(14) (Nov. 25, 2002).

9 Alexander Hamilton, "The Consequences of Hostilities Between the States" (Federalist Paper 8), *New York Packet*, Nov. 20, 1787.

10 Kennedy v. Mendoza-Martinez, 372 U.S. 144, 165 (1963).

11 Benjamin Franklin, *Historical Review of Pennsylvania* 1 (1759).

Appendix A Biographies of Technology and Privacy Advisory Committee Members and Staff

TAPAC Members

Newton N. Minow, Chairman, is Senior Counsel to the law firm of Sidley Austin Brown & Wood. He was a managing partner with Sidley & Austin from 1965–1991. He served as a U.S. Army Sergeant in the China-Burma India Theater in World War II. He served as a Law Clerk to the Honorable Fred M. Vinson, Chief Justice of the United States, and as Assistant Counsel to Governor Adlai E. Stevenson. In 1961, President John F. Kennedy appointed him Chairman of the Federal Communications Commission. Mr. Minow has served as Chairman of the Carnegie Corporation, the Public Broadcasting Service, and The RAND Corporation, and as a trustee of the Mayo Clinic. He is a life trustee of Northwestern University and the University of Notre Dame. He co-chaired the 1976 and 1980 presidential debates and is Vice Chairman of the Commission on Presidential Debates, which sponsors the debates. He has served on numerous presidential commissions. A graduate of Northwestern University, he is the Walter Annenberg Professor Emeritus there, as well as the author of four books and numerous professional journal and magazine articles and the recipient of 12 honorary degrees.

Floyd Abrams is a partner in the New York law firm of Cahill Gordon & Reindel LLP and is the William J. Brennan, Jr. Visiting Professor of First Amendment Law at the Columbia Graduate School of Journalism. Mr. Abrams has argued frequently in the Supreme Court in a large number of its most significant First Amendment cases. He graduated from Cornell University in 1956 and the Yale Law School in 1960. He was a Visiting Lecturer at the Yale Law School from 1974 to 1980 and 1986 to 1989 and the Columbia Law School from 1981 to 1985. He is a recipient of the William J. Brennan, Jr. Award for outstanding contribution to public discourse; the Learned Hand Award of the American Jewish Committee; the Thurgood Marshall Award of the Association of the Bar of the City of New York; the New York Press Club John Peter Zenger Award; the Judge Louis J. Capozzoli Award of the New York County Lawyers Association; the Democracy Award of the Radio Television News Directors Foundation; Ross Essay Prize of the American Bar Association; and many others. Mr. Abrams was Chairman of the Communications Committee of the Association of the Bar of the City of New York, the Committee on Freedom of Speech and of the Press of the Individual Rights Section of the American Bar Association; the Committee of the Freedom of Expression of the Litigation Section of the American Bar Association; and of Mayor Edward Koch's Committee on Appointments. He currently

chairs the New York State Commission on Public Access to Court Records.

Zoë Baird is president of the Markle Foundation, a private philanthropy that focuses on using information and communications technologies ("IT") to address critical public needs, particularly in the areas of health care and national security. Since joining the Foundation in 1998, Ms. Baird has developed it into an operating foundation that, in addition to its work in health care and national security, has been instrumental in working with the governments of the G-8 countries and major developing countries to establish mechanisms to address international IT policy and to enable the use of IT to achieve development goals. Ms. Baird's career spans business, government and academia. She has been senior vice president and general counsel of Aetna, Inc., a senior visiting scholar at Yale Law School, counselor and staff executive at General Electric, and a partner in the law firm of O'Melveny & Myers. She was Associate Counsel to President Jimmy Carter and an attorney in the Office of Legal Counsel of the U.S. Department of Justice. She served on President Clinton's Foreign Intelligence Advisory Board and on the International Competition Policy Advisory Committee to the Attorney General. Ms. Baird is a member of the American Law Institute and served on the congressional Commission on the Roles and Missions of the Intelligence Community. She serves on a number of private and non-profit boards of directors.

Griffin Bell joined King & Spalding as a partner in 1953 and became Managing Partner in 1958. In 1961, President John F. Kennedy appointed him to serve as a United States Circuit Judge on the Fifth Circuit Court of Appeals. He served as the 72nd Attorney General of the United States from 1977-79. He is a member of the American College of Trial Lawyers, serving as its President from 1985–86. He is also a member of the American Law Institute. Judge Bell was the initial Chairman of the Atlanta Commission on Crime and Juvenile Delinquency. During 1980, he headed the American delegation to the conference on Security and Cooperation in Europe, held in Madrid. In 1984, Judge Bell received the Thomas Jefferson Memorial Foundation Award for Excellence in Law. From 1985-87, Judge Bell served on the Secretary of State's Advisory Committee on South Africa, and in 1989, he was appointed Vice Chairman of President Bush's Commission on Federal Ethics Law Reform. During the Iran Contra investigation, he was counsel to President Bush. Judge Bell graduated *cum laude* from Mercer University Law School in 1948.

Gerhard Casper is President Emeritus of Stanford University and the Peter and Helen Bing Professor in Undergraduate Education at Stanford. He is also a Professor of Law, a Senior Fellow at the Institute for International Studies, and a Professor of Political Science (by courtesy). Professor Casper studied law at the universities of Freiburg and Hamburg, where, in 1961, he earned his first law degree. He attended Yale Law School, obtaining his Master of Laws degree in 1962. He then returned to Freiburg, where he received his doctorate in 1964. He has been awarded honorary doctorates, most recently in law from Yale and in philosophy from Uppsala. In the fall of 1964, Professor Casper immigrated to the United States, spending two years as Assistant Professor of Political Science at the University of California at Berkeley. In 1966, he joined the faculty of the University of Chicago Law School, and between 1979 and 1987 served as Dean of the Law School. In 1989, he was appointed Provost of the University of Chicago. He served as President of Stanford University from 1992–2000. Professor Casper is the author of numerous scholarly books and articles and occasional pieces. From 1977 to 1991, he was an editor of *The Supreme Court Review*. He has been elected to membership in the American Law Institute (1977), the International Academy of Comparative Law, the American Academy of Arts and Sciences (1980), the Order pour le mérite für Wissenschaften und Künste (Order pour le mérite for the Sciences and Arts) (1993), and the American Philosophical Society (1996). Professor Casper serves as a successor trustee of Yale University, a member of the Board of Trustees of the Central European University in Budapest, and a

member of the Trilateral Commission. He is also a member of various additional boards, including the Council of the American Law Institute and the Board of the American Academy in Berlin.

William T. Coleman, Jr. is a Senior Partner and the Senior Counselor in the law firm of O'Melveny and Myers. He received his A.B. *summa cum laude* from the University of Pennsylvania and his LL.B. *magna cum laude* from Harvard University, where he was an editor of the *Harvard Law Review*. He clerked for the Honorable Herbert F. Goodrich on the U.S. Court of Appeals for the Third Circuit, and for the Honorable Felix Frankfurter on the U.S. Supreme Court. He was Secretary of the Department of Transportation during the Ford Administration. He is a member of the Executive Committee of the Trilateral Commission, the Council on Foreign Relations, and the Boards of Trustees of the Carnegie Institution of Washington, the Brookings Institution, the Philadelphia Museum of Art (Vice President), and the New York City Ballet, Inc. He was a member of the Board of Directors of the National Symphony Orchestra, a Trustee of the National Gallery of Art, and an Advisory Director of the Metropolitan Opera. He is a former member of the Board of Overseers of Harvard University and of the Boards of Directors of AMAX, Chase Manhattan Bank, N.A., Chase Manhattan Corporation, CIGNA Corporation, IBM Corporation, Pan American World Airways, PepsiCo., Inc., Philadelphia Electric Company, and New American Holdings. He is the author of many scholarly articles and a fellow of the American College of Trial Lawyers, the American Academy of Appellate Lawyers, of the American Law Institute, the American Academy of Arts and Sciences, and of the American Philosophical Association. He served as President and as Chair of the NAACP Legal Defense and Educational Fund. Mr. Coleman has received the French Legion of Honor and the Presidential Medal of Freedom.

Lloyd N. Cutler is a founding partner of the law firm of Wilmer, Cutler & Pickering. He served as Counsel to Presidents Clinton and Carter; Special Counsel to the President on Ratification of the Salt II Treaty (1979–1980); the President's Special Representative for Maritime Resource and Boundary Negotiations with Canada (1977–1979); and Senior Consultant, President's Commission on Strategic Forces (Scowcroft Commission, 1983–1984). He was a member and former Chairman of the Quadrennial Commission on Legislative, Executive and Judicial Salaries, and was a member of the President's Commission on Federal Ethics Law Reform (1989). Mr. Cutler is a graduate of Yale University (B.A. 1936; LL.B. 1939) and was awarded a Yale honorary Doctor of Laws degree in 1983. He also was awarded an honorary Doctor of Laws degree from Princeton University in 1994; the Jefferson Medal in Law at the University of Virginia in 1995; the Fordham-Stein Prize, Fordham University School of Law, 1995; and the Marshall-Wythe medal of the Law School of William and Mary. Mr. Cutler was a founder and Co-Chairman of the Lawyers Committee on Civil Rights Under Law. He has served as Chairman of the Board of the Salzburg Seminar; Co-Chairman of the Committee on the Constitutional System; a member of the Council of the American Law Institute; a trustee emeritus of The Brookings Institution and a member of its Executive Committee; and an Honorary Bencher of the Middle Temple. He also has served as a director of a number of national business corporations.

John O. Marsh, Jr. is a Distinguished Professor of Law at George Mason University, concentrating on cyberterrorism and national security law. He enlisted in the U.S. Army in 1944 and was commissioned a second lieutenant at age 19. He later served in the Army Reserve and the Virginia National Guard, much of his service being in the 116th Infantry Regiment. He graduated from the Army Airborne and Jumpmaster Schools and earned Senior Parachutist Wings. He received his law degree in 1951 from Washington and Lee University and began his practice of law in Strasburg, VA. He was elected to four terms in Congress from the Seventh District of Virginia (1963–71), and served on the House Appropriations Committee. Choosing not to seek a fifth term, he resumed the practice of law. In March 1973, he returned to federal service as Assistant Secretary of Defense for

Legislative Affairs. In January 1974, he became Assistant for National Security Affairs to Vice President Ford, and in August 1974 became Counselor, with Cabinet rank, to President Ford. He chaired the Presidential Committee for the Reorganization of the U.S. Intelligence Community in 1975–76. From 1981–1989, he served as Secretary of the Army; his tenure was the longest of any Secretary in American history. Secretary Marsh has been awarded the Department of Defense Distinguished Public Service Award on six occasions, has been decorated by the governments of France and Brazil, and holds the Presidential Citizens Medal. He was selected as Virginian of the Year for 1990 by the Virginia Press Association and has received the George Catlett Marshall Medal for public service from the Association of the United States Army. He is a member of the advisory council of the Virginia Institute of Marine Science, chairs the advisory committee of Virginia Inland Port, and is a member of the Special Congressional Panel on Terrorism to Assess Federal, State and Local Response to Weapons of Mass Destruction (the Gilmore Commission).

Executive Director and Designated Federal Official

Lisa A. Davis serves as the Executive Director and Designated Federal Official of the Technology and Privacy Advisory Committee. Mrs. Davis was appointed Principal Assistant Deputy Under Secretary of Defense for Industrial Policy on December 3, 2001. Her responsibilities include world-wide industrial base management initiatives, such as E-business solutions, acquisition management improvements, and best business practices. She brings to this position extensive experience in defense contracting and acquisition policy, management, and legislation from positions in the Defense Department, industry, and Capitol Hill. She has negotiated and managed major systems acquisitions for the Army, Navy, and Marine Corps, and has held positions of increasing responsibility in the office of the Secretary of Defense. Mrs. Davis graduated with honors from Ball State University, and earned the title Certified Contracts Manager from the National Contract Management Association/Defense Systems Management College.

Reporter

Fred H. Cate is the reporter for TAPAC. He is a Distinguished Professor and director of the Center for Applied Cybersecurity Research at Indiana University. He appears regularly before Congress, government agencies, and professional and industry groups on privacy, security, and other information law matters. Professor Cate directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities, and was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He is a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams, a member of Microsoft's Trustworthy Computing Academic Advisory Board, and a member of the board of editors of *Privacy & Information Law Report*. He has led projects for the American Enterprise Institute, The Annenberg Washington Program, and the Brookings Institution. He is the author of many articles and books, including *Privacy in the Information Age*, *Privacy in Perspective,* and *The Internet and the First Amendment*. A member of the American Law Institute and a Senator and Fellow of the Phi Beta Kappa Society, he received his J.D. and his A.B. with Honors and Distinction from Stanford University.

APPENDIX B TAPAC WITNESSES

The Hon. E.C. Aldridge, Under Secretary of Defense (Acquisition, Technology and Logistics)

Lieutenant General Keith B. Alexander, Deputy Chief of Staff for Intelligence, U.S. Army

Stewart Aly, Associate Deputy General Counsel, Department of Defense

Maureen Baginski, Executive Assistant Director of Intelligence, Federal Bureau of Investigation

Stewart Baker, Attorney at Law, Steptoe and Johnson, LLP

Jennifer Barrett, Chief Privacy Officer, Acxiom

Jerry Berman, President, Center for Democracy and Technology

John Brennan, Director, Terrorist Threat Integration Center

Scott Charney, Chief Trustworthy Computing Strategist, Microsoft Corp.

Gary Clayton, Founder and CEO, Privacy Council, Inc.

William P. Crowell

Michael de Janes, General Counsel and Secretary, ChoicePoint

Robert L. Deitz, Deputy General Counsel (Intelligence), Department of Defense

Jim Dempsey, Executive Director, Center for Democracy and Technology

Viet Dinh, Professor of Law, Georgetown University Law Center

Brigadier General George R. Fay, Commanding General, U.S. Army Intelligence & Security Command

Dr. Usama Fayyad, President, DMX Group; Chairman, Revenue Science, Inc.

Dr. Edward W. Felten, Professor of Computer Science and Director of the Secure Internet Programming Laboratory, Princeton University; Co-Chairman of DARPA Information Science and Technology Advisory Board

Dan Gallington, Senior Research Fellow at the Potomac Institute for Policy Studies

The Hon. Governor James S. Gilmore, III, Chair, Congressional Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction

Jamie Gorelick, Partner, Wilmer, Cutler & Pickering

Jeff Green, Senior Attorney, Standards of Conduct Office, Department of Defense

Carol Haave, Deputy Under Secretary of Defense (Security and Information Operations)

Dr. David Jensen, Research Assistant Professor of Computer Science and Director of the Knowledge Discovery Laboratory, University of Massachusetts Amherst

Jeff Jonas, Chief Scientist and Founder, Systems Research & Development

Dr. Takeo Kanade, U.A. Helen Whitaker University Professor of Computer Science and Robotics, Carnegie Mellon University

Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security

Dr. Thomas H. Killion, Acting Deputy Assistant Secretary for Research and Technology/Chief Scientist, Department of Defense

George B. Lotz, II, Assistant to the Secretary of Defense (Intelligence Oversight)

Teresa Lunt, Principal Scientist and Area Manager of Security Group and Area Manager of Theory Group, Palo Alto Research Center

The Hon. Paul McHale, Assistant Secretary of Defense for Homeland Defense

Judith A. Miller, Williams & Connolly

Lieutenant Colonel Ronald K. Miller, United States Air Force

Vahan Moushegian, Director, Privacy Office, Department of Defense

The Hon. Representative Jerry Nadler (D-N.Y.)

Major General Paul D. Nielsen, Commander, Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio

Sue Payton, Deputy Under Secretary of Defense (Advanced Systems & Concepts)

Dr. Gregory Piatetsky-Shapiro, President, KDnuggets

Dr. Robert Popp, Special Assistant to the Director for Strategic Matters, DARPA

Vito Potenza, Acting General Counsel, National Security Agency

Michael R. Ramage, General Counsel, Florida Department of Law Enforcement

Thomas M. Regan, Executive Director for Privacy and Regulatory Affairs, LexisNexis

Martha Rogers, Partner, Peppers & Rogers

Paul Rosenzweig, Senior Legal Research Fellow, Heritage Foundation

Dr. Nils R. Sandell, Jr., President and CEO, ALPHATEH, Inc.

Brian Sharkey, Senior Vice President, Advanced Systems and Concepts, Hicks & Associates

Jeffrey H. Smith, Arnold & Porter

Jim Smyser, Associate Deputy General Counsel (Military Personnel and Reserve Policy)

David Sobel, General Counsel, Electronic Privacy and Information Center

Jay Stanley, Communications Director, American Civil Liberties Union

James B. Steinberg, Vice President and Director, Foreign Policy Studies, Brookings Institution

Dr. Latanya Sweeney, Director, Laboratory for International Data Privacy, Carnegie Mellon University

Captain David C. Taylor, United States Navy, Chief, J6 Director's Action Group

Dr. Anthony J. Tether, Director, Defense Advanced Research Projects Agency

Stephen Thayer, Deputy Director, Office of National Risk Assessment, Department of Homeland Security

Michael Vatis, Executive Director, Markle Foundation Task Force on National Security in the Information Age

Allan Wade, Chief Information Officer, Central Intelligence Agency

The Hon. Senator Ron Wyden (D-Ore.)

The Hon. Michael W. Wynne, Acting Under Secretary of Defense (Acquisition, Technology and Logistics)

Lee M. Zeichner, President, Zeichner Risk Analytics, LLC