

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

May 20, 2002

The Honorable Donald L. Evans
Secretary of Commerce
14th Street and Constitution Avenue, NW
Washington, DC 20230

Dear Mr. Secretary,

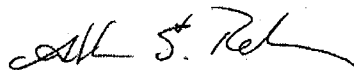
I have the honor to transmit the final draft of a report of the Computer System Security and Privacy Advisory Board (CSSPAB), adopted at its March 2002 meeting. The Board was created by the Computer Security Act of 1987 to "(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy; (2) to advise the Bureau of Standards [now the National Institute of Standards and Technology] and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and (3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress."

The enclosed draft report reflects the results of inquiries and discussions of the Board over the past year. In summary, the Board found substantial opportunities for improving the way the privacy responsibilities of Federal agencies are administered and a need for improvements and clarifications in policy guidance, if not changes in law, to reflect changes in technology since enactment of the Federal Privacy Act in 1974.

The Board plans to publish the report as an exposure draft on its web site to give interested parties, including those who participated in its meetings, an opportunity to comment. We will then revise the report as necessary to reflect those comments.

We hope and trust that the Board's advice can make a constructive contribution to the security and privacy of Federal information systems and to public confidence in those systems, and we stand ready to provide whatever additional assistance we can to advance those causes.

Sincerely,



Franklin S. Reeder
Chairman

Enclosure

cc: The Honorable Mitchell Daniels
Director of the Office of Management and Budget

The Honorable Arden L. Bement, Jr.
Director of the National Institute of Standards and Technology

Exposure Draft

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD FINDINGS AND RECOMMENDATIONS ON GOVERNMENT PRIVACY POLICY SETTING AND MANAGEMENT

May 2002

OVERVIEW

The Computer System Security and Privacy Advisory Board (CSSPAB) determined in September 2000 that privacy would be included as one of the Board's initiatives under its new strategic plan. The Board addressed privacy issues in subsequent board meetings, including presentations from leading private sector privacy experts, the Office of Management and Budget, and government privacy officers and policymakers. In order to achieve a more structured focus, the CSSPAB devoted two full days of its June 19 and 20, 2001, quarterly meeting, hosted by The John Marshall Law School in Chicago, Illinois, to address issues related to government data privacy. The Board heard from thirteen government and industry experts. The minutes of this meeting and the privacy sessions as well as accompanying presentations are available at the CSSPAB Web site, <http://csrc.nist.gov/csspab>.

For these sessions, the Board's focus was on two broad questions important to the Federal government:

1. **Government Privacy Policies** – are government privacy policies adequate in light of technological, societal and other policy changes and influences?
2. **Government Privacy Management** – can improvements be made to Federal agencies' business processes and use of technology in support of law, regulations and privacy policies?

In addition to hearing from the expert participants who addressed these issues at the Chicago meeting, CSSPAB Chairman Franklin Reeder and board member John Sabo had follow-on fact-finding discussions in the Fall of 2001 with a number of government privacy officers in major civil and Department of Defense (DOD) agencies and Departments to further explore issues raised by the Chicago speakers.

In the aftermath of the terrorist attacks of September 11, 2001, the government's critical focus on policies and operational plans necessary to improve homeland security further highlight the need to address the questions raised in the Board's inquiries on data privacy. For example, the Patriot Act authorized additional data collection and data processing authorities for law enforcement purposes in order to provide enhanced security and protection against terrorists and terrorist acts. Further, as this report is written, very serious analysis is underway in both the public and private sectors regarding increased interconnection of information systems, sharing of data, and the aggregation, warehousing and processing of data from both private sector and government sources in ways contemplated at the time the Privacy Act was written, but now requiring consideration in light of the events of September 11th.

With these additional authorities and the increased use of information systems for homeland security, the fundamental issues identified by the CSSPAB as a result of its inquiries into government privacy and privacy management deserve accelerated attention. However, even as a new national discussion emerges regarding the appropriate policy balance between homeland

security requirements and data privacy, the government's collection, processing, and disclosure of personal information under previously established authorities and practices has continued. With the migration toward e-Government services, greater demands will be placed on the government's privacy policies and systems. As virtually all of the public opinion polling data suggest, the public's willingness to use electronically enabled transactions process (e-government or e-commerce) depends in large measure on their confidence that information that they disclose will be safeguarded.

It is the Board's belief that changes in technology, the privacy management challenges stemming from expanded e-government services, the accelerated interaction of networked information systems within and across critical infrastructure boundaries, and the extended, routine exchange of data by government and commercial sources -- all mandate immediate and serious attention to Federal government's data privacy policies and operational controls. This focus will also help ensure that a proper balance is struck between privacy and homeland protection efforts.

Based on its examination of these issues, the Board has determined that a number of steps need to be taken by the Federal government with respect to both privacy policy and privacy management. These steps are documented in the Board's recommendations.

ISSUES RAISED IN CSSPAB'S TWO-DAY PRIVACY MEETING JUNE 2001

In the CSSPAB's June meeting, the Board heard from a number of speakers addressing privacy issues. Minutes of this meeting, including general summaries of the privacy sessions, as well as accompanying presentations, are available at the CSSPAB Web site, <http://csrc.nist.gov/csspab>.

A number of important issues were raised for discussion, including:

- free speech and privacy in telecommunications, critical infrastructure protection, e-government services, and online access to public records;
- the impact of private sector e-business practices and Web-related technologies;
- new private sector technologies, tools and standards which have relevance both to government privacy policies and operational systems;
- online access to public records, online court records, computer-accessible government databases and the rise of identity theft;
- the potential need for a Federal privacy agency;
- implications for government of efforts to regulate commercial privacy practices, such as requirements for notice and choice and the impact on the expansion of "routine use" determinations by agencies;
- advances in data sharing technology and their implications for privacy;
- adequacy of the Federal Privacy Act in today's complex environment;
- the appropriate balance between consumer protection and risk management;
- changes in the private sector which are affecting liability with respect to data protection and privacy;
- the role of risk exposure and insurance in setting government's privacy standards and government employee liability for security and privacy failures;

- records linkages, including person-specific data collected under federal auspices and used to develop statistical information and carry out non-government research projects;
- identification of criteria for “best practices” in data stewardship; and,
- the use of audits as part of a system to ensure appropriate data privacy

Although the Board did not address the merits of specific recommendations made by the individual experts who presented, it is clear that the scope and complexity of the issues they have raised require serious, coordinated attention from government policymakers.

ISSUES RAISED IN DISCUSSIONS WITH GOVERNMENT PRIVACY OFFICERS AUGUST 2001

As a follow up to the June Board meeting, members of the CSSPAB met with a number of Federal privacy officers from major civil and DOD agencies and Departments to discuss issues raised at the June meeting. Issues addressed included how the Privacy Act was being administered, including adequacy of guidance and implementation and the state of the Privacy Act itself — is it adequate given technology used today such as extended networks and virtual databases, data integration, data aggregation, and increased sharing of data?

The Board members identified a number of issues of concern:

Terminology and Definitions -- most privacy discussions don't start from the same definitions; components of privacy (such as what constitutes the boundaries of a “system”) need to be defined more clearly (and in consonance with agency statutes and regulations) across government, enabling greater clarity, specificity and structure around privacy discussions and better cross-government policy development.

Privacy Act Review -- review of the adequacy and relevance of the Privacy Act should be undertaken, to determine whether modifications to the Act are required, given the numerous changes affecting privacy which have occurred in the almost three decades since the Act was passed.

Technological Change -- There has been a migration from legacy applications and defined systems of records, to distributed processing systems with linkages to data. This architectural transformation results in a requirement for analysis and guidance if agencies are to properly understand and manage privacy in today's environment. No one in government is addressing how these technological changes affect privacy practices across government agencies.

Data Ownership -- The important distinction between personal information maintained directly by the Federal government and personal information over which government has control (but which the government does not maintain) is not addressed by the Privacy Act. For example, in recent years, the Federal government has mandated private sector collection of new hire data. However, the government does not have direct control of this data collection, and its responsibilities under the Privacy Act concerning such data should be clarified.

Role of CIO's in Data Privacy -- The responsibilities of agency CIO's do not include privacy in parallel with their responsibilities for information security. As a result, there is often a disconnect between information security decision-making, budgeting and communications and similar matters related to privacy, despite the fact that privacy requires close coupling with security services.

Organizational Authority and Management -- Leadership and points of contact for privacy in various agencies display disparate levels of oversight, authority and management. The Privacy

Act requires a "senior official" at agencies, but not all have been named. The wide disparity of organizational location and responsibilities of the "senior officials" has the potential to hamper agency compliance with the Privacy Act and to create inconsistent privacy policy development and management from agency to agency. Although rote uniformity is not necessarily helpful across government given the enormous differences among agencies in mission, responsibilities and resources, it may be useful to examine organizational privacy policy-setting, leadership and management to determine whether common improvements are needed.

Leadership -- There is no clear point of leadership across the Federal government for privacy generally, let alone for the Privacy Act. OMB is the de facto government body to provide such leadership, but to perform its functions effectively, OMB needs to provide more active attention and direction, and have adequate staff to carry out its responsibilities.

Cross-government Vehicle for Privacy Communication and Coordination -- mechanisms have existed in the past, such as the Security, Privacy and Critical Infrastructure Sub Committee of the CIO Council which held promise as a cross-Agency forum for privacy issues; outside government, the Privacy Officers Association and American Society of Access Professionals provide professional networking and education. However, a vehicle is badly needed within government to promote communication, coordination, policy and best practices development for agencies.

BOARD RECOMMENDATIONS

Following discussions over several board meetings, the expert presentations at the June privacy meeting, and dialogue with senior Federal privacy officials, the Computer System Security and Privacy Advisory Board believes that a number of actions should be taken to address the major issues documented in this report.

The Board believes that many of the recommendations can be undertaken with minimal cost or effort on the part of government, particularly those involving improving the development of privacy definitions and policies and the establishment of mechanisms to improve internal coordination and lines of communication among Federal agency privacy officials.

Specifically the Board recommends the following steps:

1. Document and strengthen privacy management practices across the Federal government by:
 - a. Identifying and categorizing all privacy officials across Federal government departments and agencies, identifying grade and organizational level, location within the agency hierarchy (i.e., reporting chain), assigned authorities and responsibilities, staff size and composition (e.g., number of attorneys, specialists, and support personnel), and other relevant factors, in order to develop a complete picture and better understanding of the Federal privacy management infrastructure.
 - b. Publishing a one-time report, which examines differences from agency to agency in light of the information and issues above.
 - c. Establishing an interagency committee or council of privacy officials to improve networking, cross-government communications, policy setting, and sharing of best practices, and to enhance opportunities for professional development.
 - d. Establishing a formal working relationship between privacy officials and agency CIO's (where that does not already exist), given the interdependence of information systems, privacy and security.
 - e. Chartering the privacy officials committee or council cited above, working with OMB, to develop an agenda for promoting improvements in privacy practices and policy across all agencies.

- f. Creating a set of government-wide, standard privacy definitions that fully reflects statutory requirements set forth in the Privacy Act and other statutes, and identifies where there are definitional overlaps or conflicts among the statutes.
2. Perform an examination of national systems of records and databases, public-private sector data disclosures, data matching systems, data exchange agreements and systems, and data linkages in order to develop a complete inventory of systems which contain or process information considered private under one or more statutes, and to develop risk management assessments and provide recommendations on changes needed to the Privacy Act and other statutes and agency regulations to eliminate conflicts and improve agency adherence to such requirements. This effort should include:
 - a. Examining those databases having linkages among Federal, state, and local government and those databases having linkages to private sector systems;
 - b. Addressing notice, choice and consent issues in the light of e-Government initiatives (to support electronic transactions with companies and members of the public) and increasing interaction among Federal and non-Federal systems, in part to ensure that consistent policies are presented to the public on privacy choices across agencies.
3. Implement an ongoing mechanism to keep abreast of and evaluate emerging private sector policies, technologies, risk management models, and operational systems and practices to evaluate their value to and impact on the government, and to employ them as appropriate.
4. Create mechanisms to ensure that those government officials responsible for the protection of private information understand and can accommodate, to the extent permitted by statute and regulation, the needs for data sharing and data matching of law enforcement agencies seeking to enhance homeland security

The Board does not make a recommendation as to which agency or organization should carry out these actions. The Board notes that the Office of Management and Budget 's responsibilities include information privacy both under the Privacy Act of 1974 and the Paperwork Reduction Act as amended, but also recognizes that OMB does not have the resources to sustain the level of effort required to carry out these actions over a long period of time. The Board believes that it may be helpful for OMB to explore the model used in the mid 1990's, when it established and managed the work of the cross-agency Benefit Systems Review Team, which brought together government experts from multiple agencies to examine needed improvements to Federal benefits systems (and which also addressed privacy issues to a limited degree). However, because the support of OMB is critical to the success of the re-examination of privacy policy and management recommended by the Board, we urge OMB to initiate a process by which the Board's recommendations can be prioritized and carried out.

Finally, the Board notes that the Government enjoys the leadership and expertise of a number of officials and policy makers who serve as privacy officials and as managers of agency privacy and disclosure policies, and who bring years of experience and management skill to these issues. They are most capable, and we believe most willing, to address the many privacy challenges facing government today and, as a starting point, need only a serious government-wide charter and the support of OMB and senior Agency executives to begin this work.