ROLE OF THE CHIEF PRIVACY OFFICER

Statement of John P. Fanning before the Information Security and Privacy Advisory Board, Rockville, Maryland, June 7, 2005.

I am John Fanning, and appear before you as a citizen with an interest in privacy and a special interest in seeing that the Federal government has effective organization and procedures to address privacy issues. I retired in July of last year from the U.S. Department of Health and Human Services (HHS), where I had spent many years working on privacy issues, the last seven as the first Privacy Advocate of the Department.

This Board has been a thoughtful commentator on the structural and organizational aspects of attention to privacy. The subject is complex and needs continuing attention, as suggested by your September 2002 recommendations on government privacy policy setting and management.

I will describe the organizational structure at the Department of Health and Human Services as I recall it. I will offer some observations on existing and proposed approaches to getting Federal agencies to organize themselves to address the serious societal issues raised by the collection and use of personal information.

HHS – The Agencies

Please note that the major attention to data collection and use in a large department is within the operating agencies. In HHS, for example, the Center for Medicare and Medicaid Services (CMS) has records of perhaps 40 million Medicare beneficiaries, and the Administration for Children and Families (ACF) manages the child support enforcement system and receives information about all employed people. Those agencies design and maintain data systems. At the same time, the Departmental management apparatus – the Office of the Secretary in the case of HHS – includes staff offices which also have certain oversight, review, and policymaking responsibilities for these data systems.

HHS – Office of the Secretary

In HHS the privacy structure at the Office of the Secretary level is a three-cornered hat:

- Management of the Privacy Act is in the hands of the Department Privacy

Officer, in the Office of the Assistant Secretary for Public Affairs. The Privacy Act Officer is also the Department's Freedom of Information Officer. The operational work (e.g., preparation and publication of system notices) is done at the agency level.

- There is a Privacy Advocate, in the Office of the Assistant Secretary for Planning and Evaluation (the policy office of the Office of the Secretary). That official provides technical help on specialized issues, and has hortatory and review functions. Located in an office with review functions for many Department policies (such as regulations, and proposals for new legislation), that official has an opportunity to address privacy issues as they come up in those processes. There is no staff beyond the individual official.

- The Chief Information Officer (CIO) is in the Office of the Assistant Secretary for Budget, Technology and Finance. That office includes the Office of Information Security Development and Implementation, which was given responsibility under the E-Government Act of 2002 for management of the privacy impact assessment (PIA) process and in making policy for web sites.

  And the CIO was identified as the senior official for privacy in accord with OMB's directive of February of this year to have such an official. (Memorandum, *Designation of Senior Agency Officials for Privacy*, February 11, 2005). That office also has responsibility, *inter alia*, for managing activities under the Paperwork Reduction Act of 1995, the Computer Matching and Privacy Act of 1988, the Computer Security Act of 1987, the Government Information Security Reform Act (GISRA), and OMB Circular A-130.

Earlier, in 1999, when the President and OMB commanded that agencies have a Senior Official for Privacy Policy the Secretary designated the Assistant Secretary for Planning and Evaluation, probably because the Privacy Advocate was located in that office. That official did not do anything different from the existing data policy and privacy functions of the office as a result of the appointment.

In my experience, despite apparent overlap among these three functions, the system worked well, largely because of mutual respect and regular communication among the career officials involved. For example, in carrying out the E-Government Act of 2002, the Privacy Officer and Privacy Advocate were closely involved in the CIO's design of the standards for PIAs, and they reviewed

the submitted PIAs.

The Operating Level

But again, I note that the design and management of data systems, and perforce the major and persistent policy choices about them, are made by program officials at the operating level.

Thus, it is important to emphasize that privacy is everyone's responsibility. This goes beyond the traditional cliché sense of that incantation (although it is important and true in that sense too). Since the practical business of designing data systems and of making policy for use of information resides with program officials in operating units of an agency, it is there that privacy must be taken into account in the first instance. The systems are often complicated. It is there that the true implications and potential of collecting information can be understood. The officials at that level must be attuned to the privacy implications of what they are doing, and not expect that some specialist official will later make it turn out right.

Some of the significant privacy issues will arise not from direct agency collection of personal information, but from agency activities – funding, regulatory commands, exhortation, or other mechanisms – that stimulate others, such as state and local governments and private entities, to collect personal information. Proposals for agency action in this arena require quite as much attention as proposals for direct Federal collection of information.

For example, the Department of Health and Human Services has set out, through its Office of the National Coordinator for Health Information Technology, to provide strategic direction for development of a national interoperable health care system, and to address barriers to the widespread adoption of electronic health records. Such an undertaking requires major attention to privacy, both within the specific developmental activity, and from the regular privacy apparatus of the Department.

The operating agencies of HHS do have a long history of careful, systematic attention to privacy, and there have been dedicated privacy staffs. The National Center for Health Statistics shares with other statistical agencies the preoccupation with, and commitment to, safeguarding its identifiable information, as a *sine qua non* of continuing ability to get it. It has, for as long as I can recall, had a senior person dedicated to privacy and confidentiality, with a staff.

The Center for Medicare and Medicaid Services, heir to the privacy awareness of the Social Security Administration, has a Privacy Rights and Protection Staff in its Center for Beneficiary Choices, and a Beneficiary Confidentiality Board composed of senior officials.

Those of us who have been practitioners of generic privacy owe much of our education to the dedicated people who had long tended to the issue in specific programs.

Oversight and Review – The Privacy Official

That said, it is equally clear that there must be someone at a higher level who has privacy as a sole responsibility – a cause, if you will – and who

- has a formal role in policymaking,
- is outside the immediate design process,
- located at a sufficiently high level to have an overview and bring wide experience to bear, and
- has access to high-level officials.

That official – with adequate staff – should be available for consultation and advice in advance of the design of systems, and in advance of seeking formal approval at a high level. This is the role of the privacy official as a helper and source of technical expertise, to complement and develop skills and expertise at the system development level. That official can educate in a systematic way the officials who design systems; hopefully that education will not be by way of conditioning through rejections at the end of the design process.

Such an office should also be able to conduct and commission research and otherwise think about the issues more broadly, and not merely in the context of protecting people against harm in this or that data collection. These topics are getting more complicated – partially because of the laws, but mostly because of the technology – and there ought to be a staff that can become expert at the business of data protection. In addition, there are other organizations which have dedicated people or staffs (e.g., Federal agencies like the Federal Trade Commission and the Department of Commerce, the data protection staff of the European Commission, and foreign data protection officials) and an agency needs someone who can relate to them.

The precise location and structure of privacy oversight depend on the size and

structure of an agency, and the nature of its data systems. But the official must be at a sufficiently high level to be able to raise concerns well above the level of the proponents of a particular data system, and ideally, to the head of the agency. Let me address some of the existing requirements for privacy officials.

The Agency Official

The February OMB guidance requires the head of each agency to designate a senior official who is to

> have overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

The CIO is suggested as the official. This suggestion needs examination. In some instances, to give the CIO these responsibilities would require reorganization that would have implications beyond privacy protection.

In addition, the intellectual and organizational framework of these offices is oriented toward technology issues, and particularly the subset of data protection that is security. It is important that the privacy issues we are discussing here receive broad policy consideration, from many perspectives, and not be seen, for example, as ancillary to security. Some such offices do these broad review tasks very well, but the issue of placement does need further attention.

Chief Privacy Officer Requirement

Some of the functions for a Chief Privacy Officer required by section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Pub. L. No. 108-447), are reasonable, but in my view a statute with this level of detail cannot effectively structure a privacy protection organization across the great range of Federal agencies. Their needs vary because they differ greatly in mission, organization, size, and types of personal information gathered.

Broad assurance responsibilities are appropriate – this is the review and hortatory function that existing privacy officials often have. But, for example, should it be the Chief Privacy Officer who prepares a privacy impact assessment, as the statute requires, or should it be the developer of the data system? Likewise, the training and educating of employees on privacy and data protection policies might

in some small agencies be an appropriate role for a Chief Privacy Officer, but in others this might well be better designed, arranged, and conducted at an operating level.

In addition, the detailed requirements for purchasing third-party review are not appropriate.

The provision also requires a report to Congress; it picks up the language in the Homeland Security Act of 2002 (sec. 222) that established the Chief Privacy Officer in the Department of Homeland Security. ("(5) preparing a report to Congress on an annual basis on activities of the Department that affect privacy including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.")

It might be acceptable to assign the task of writing a report to this office, but it is not appropriate that an official of the Department should send such a report to the Congress independent of the regular management of the agency. The privacy officer should be integrated into the normal structure of the Department, and not be seen as an independent review apparatus. The privacy official must be seen as a source of help and guidance, not as a potential tattle-tale. And it is the head of the agency who should confront the issues that would be raised in such a report.

#

June 6, 2005

John P. Fanning