



## ***Information Privacy in the Federal Government: Moving Your Agency Forward While Meeting Your Privacy Commitments***

### **Introduction**

Everyday U.S. government departments and agencies collect, process, transmit or store personally identifiable information (“PII”)<sup>1</sup> in the normal course of daily operations. This PII can be basic information such as a person’s name and address or much more sensitive such as a person’s social security number, passport number, medical information, or financial information. The most highly sensitive PII relates to the combination of information about an individual or individuals: relationships between individuals, historical transaction information, or case information about individuals. PII may pertain to government employees, individuals served by a particular department or agency, or people connected with those individuals (e.g., relatives). This information is entrusted to your department or agency with the expectation that you will maintain its privacy in accordance with the commitments made by the Executive Branch of the Federal Government. These commitments are outlined both through federal legislation, Office of Management and Budget Circular A-130, NIST guidance, as well as individual department directives and policies.

The purpose of this paper is to review the fundamental requirements that all agencies need to satisfy, and present an approach to effectively and efficiently manage the privacy program for your agency while continuing to move the work of the agency forward. The consequences of not properly managing your privacy program will likely result in the perception of information misuse and cause

- Legal action from privacy advocacy groups;
- Reputation damage and scrutiny for your agency and leadership;
- Relentless critical mainstream media coverage;
- Potential Congressional or GAO inquiries; and,
- At worst, the agency’s program is delayed or shut down.

If privacy commitments are ignored or risks are not properly managed, it is not a question of if such an outcome will occur, but a question of when it will occur.

### **A History of Privacy Concerns**

Protecting the privacy of information is not a new concept. However, advances in technology have facilitated the mass collection, storage, matching and mobility of information. In addition,

---

<sup>1</sup> PII is defined as any data element that can be attributed to a specific person.

these same advances also help facilitate the ease with which PII that is lost or stolen can be misused for identity theft, of the individual.

The GAO has conducted numerous reviews of various privacy aspects at agencies that resulted in critical reports and testimony with titles such as:

- *“Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information”* testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate.
- *“DHS Privacy Office Has Made Progress but Faces Continuing Challenges”*
- *“Health Information Technology: Efforts Continue but Comprehensive Privacy Approach Needed for National Strategy”* before the Subcommittee on Information Policy, Census, and National Archives Committee on Oversight and Government Reform U.S. House of Representatives.

It is reasonable to expect that additional GAO reviews will occur in the future and your agency may be the focus and required to publicly defend your privacy program.

The public continues to be increasingly concerned about the privacy of their PII. Privacy Rights Clearinghouse reports that there have been over 1,200 incidents of PII loss or theft at U.S. organizations from January 2005 – May 12, 2009 affecting approximately 262 million individuals. A number of these incidents received extensive prime time media coverage. In the recent past, compromised PII was reported by various agencies including the FAA and the U.S. Army, the U.S. Air Force, Department of Agriculture and the Transportation Security Administration. Perhaps the most publicized incident of all time occurred at the Department of Veterans Affairs in May 2006.

### **The Legal Landscape**

In order to define what an individual should be able to expect in terms of the privacy of the information entrusted to the federal government, the following Federal laws were enacted and apply to all agencies. These laws are more inclusive than regulations that pertain to the private sector, and must be strictly adhered to.

#### *Privacy Act of 1974*

The Privacy Act of 1974 is the landmark law that establishes the statutory foundation for modern Fair Information Principles. The Act requires agencies to:

- Limit PII to what is “relevant and necessary”
- Collect PII directly from the individual wherever possible
- Maintain the accuracy, currency and completeness of PII
- Limit disclosure of PII to those who need for appropriate purposes

- Allow access and correction of PII
- Secure systems containing PII

The E-Government Act

This Act requires agencies to conduct a Privacy Impact Assessment (“PIA”) before:

- Developing, procuring, or significantly changing IT systems that collect, maintain, or disseminate information in identifiable form from or about members of the public;
- Initiating a new electronic collection of information in identifiable form for ten or more persons; and
- Agencies must post a privacy policy on their websites. This privacy policy must be in both text form that can be read by a website visitor as well as in P3P format that can read by the website visitor’s browser.

PIAs are a fundamental component of an effective information privacy program. PIAs must be specifically address:

- *What* PII is to be collected;
- *Why* is the PII being collected;
- *What* are the intended uses of PII;
- *With whom* the PII will be shared;
- *What* opportunities are available to the person to decline to provide PII or provide consent;
- *How* the PII will be secured;
- *Whether* a system of records is being created under the Privacy Act; and
- *Analysis of* information life cycle and of choices made

*Source: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22, September 26, 2003*

The Consolidated Appropriations Act of 2005

This Act requires:

- A biennial independent privacy audit overseen by the Inspector General that:
  - Ensures the accuracy of each agency’s description of the use of information;
  - Determines the effectiveness of the actual privacy and data protection procedures;

- Ensures compliance with all stated policies, laws and regulations; and
- Ensures that all technology used allow for continuous compliance auditing.

The Federal Information Security Management Act of 2002 (FISMA)

FISMA is included in Title III of The E-Government Act of 2002 and is a comprehensive framework for ensuring: the effectiveness of information security controls within the federal government; requires government-wide management and oversight of information security risks; development of minimum security controls; oversight of agency information security; the use of commercially developed information security products and agency decision making regarding the specific information security solutions chosen.

**Privacy Effectiveness Series™**

Effective privacy programs require a focused approach that couples a holistic view with pragmatic action plans. *How does your privacy program measure up? Would external privacy advocates agree (e.g., Electronic Privacy Information Center or the Center for Democracy & Technology)?*

The Privacy Effectiveness Series™ is a structured progression to assess your privacy program ensuring that every dollar invested provides value and contributes to achieving the agency's overall mission. The Privacy Effectiveness Series™ is modular and customizable recognizing that privacy programs are at different levels of maturity. While using the same basic framework, a modular approach allows for the best match of an agency's needs to focused activities in the areas requiring enhancement. Major modules in the Privacy Effectiveness Series™ include:

Current State Diagnostic – to understand if there are areas of the privacy program that need improvement, a current state diagnostic that includes all major privacy program activities is a necessary first step. Included in this activity is a review of:

- Policies and Procedures
- How privacy is embedded in the systems and business process development life cycle
- Training
- On-going Communications
- Privacy Impact Assessment Process
- Website Privacy Statement
- Incident Response Plan
- Legal compliance program

The current state and supporting infrastructure will then be compared to expected privacy practices and legal requirements and areas for improvement will be identified.

Creation of a Heat Map – the heat map is a matrix that summarizes the current state against the desired state in an easy to understand overview that visually highlights high risk areas in red, moderate risks in orange and low risks in yellow.

Privacy Improvement Plan – working with agency stakeholders this module will focus on the preparation of a practical and actionable privacy improvement plan that when executed will demonstrate effective management of privacy risks.

Implementation of the Privacy Improvement Plan – effective implementation of the privacy plan is essential, it will ultimately affect if your program is successful or not. Assistance by privacy experts can help ensure that your privacy improvement plan is implemented effectively, on schedule and without interrupting operations or consuming government employee resources that are already committed to other important efforts.

These proactive measures will help ensure that:

- your privacy risks are proactively and appropriately managed;
- projects with privacy considerations move forward on-time and on-budget;
- your agency achieves its objectives; and
- the chances of your agency becoming the next privacy incident headline are reduced.

Monitoring – on-going monitoring of the privacy program ensures the agency’s privacy goals and legal requirements are continuously satisfied and any necessary enhancements can be made before a problem occurs.

### **About Navigate LLC**

Navigate LLC is a business consultancy that is focused on providing pragmatic, comprehensive high value strategic and tactical information privacy advisory services to the Federal government and commercial sectors. Navigate was founded by Chris Zoladz who most recently served as the Vice President of Information Protection & Privacy at Marriott International, Inc. for the past 10 years.

For more information on how Navigate LLC can assist your agency, please call 240-475-3640 or send an email to [governmentprivacy@navigatellc.net](mailto:governmentprivacy@navigatellc.net).

© Navigate LLC 2009. Privacy Effectiveness Series™ is a trademark of Navigate LLC.