



*Privacy Office*

# Report to Congress

*April 2003 – June 2004*



**Homeland  
Security**



**Homeland  
Security**

## **Privacy and Protecting Our Homeland**

“To secure the homeland better, we must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy.”

### The National Strategy for Homeland Security

*Preserving our Freedoms, protecting America ... We secure our homeland.*

Objective 7.1: Protect confidentiality and data integrity to ensure privacy and security.

*Protecting vital and sensitive information, thus ensuring the privacy of American citizens, is important to the safety of the Nation. We will ensure the technologies employed sustain, and do not erode, privacy protections relating to the collection, use and disclosure of personal information. We will eliminate inappropriate access to confidential data to preserve the privacy of Americans. We will maintain an appropriate balance between freedom and safety consistent with the values of our society.*

U.S. Department of Homeland Security Strategic Vision



# Homeland Security

Honorable Members of Congress, fellow Americans, and neighbors around the globe:

It is my great honor to submit to the United States Congress a report on the first year of the operations of the Privacy Office at the Department of Homeland Security. I am particularly pleased to have held this role during the Department's first year at a time when, under the tremendous leadership of Secretary Tom Ridge, we seized the opportunity to promote new and lasting awareness of the responsible handling of personal information about citizens and visitors to our country.

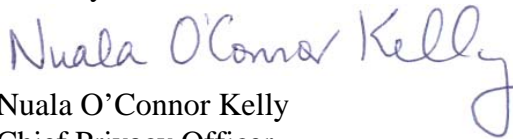
The responsible stewardship of personal information is fundamental to the Department's successful achievement of its mission. This mission is not only to protect our people and our homeland; it is to protect our way of life. Personal privacy is central to that way of life. Privacy is a core value, universally recognized, and a value long recognized in American law and jurisprudence. Because privacy is so essential to our way of life we recognize that the protection of privacy, of the very dignity and autonomy of the individual, is not a value that can be added on to this or any other organization as an afterthought. Thus, I am so pleased that the Privacy Office has been operational within the Department of Homeland Security from its earliest days. We will continue to work to ensure that privacy is woven into the very fabric of this organization as a guiding principle and value.

Our accomplishments over the first year of the Department's history are a demonstration of Congressional and Presidential foresight in embedding privacy protection into the security mission of the Department of Homeland Security. I believe that our work is testament to the commitment of our leadership and dedicated staff throughout the agency.

I also believe we have made our influence felt outside the walls of the Department, both at home and abroad, by listening to privacy concerns and by responding in positive, constructive ways. This will continue to be accomplished by consulting closely with Congress, with our colleagues across government, with representatives of the private sector, and with our counterparts in the international community.

I look forward to continuing to work within the Department to build the Department of Homeland Security into a model for the protection of our homeland and also for the protection of the privacy of all people.

Humbly submitted,

  
Nuala O'Connor Kelly  
Chief Privacy Officer

## Privacy -- Part of the Department's Mission

*"We must and we will be careful to respect people's privacy . . . Terrorists hide among us and use our freedom against us, but they will find fewer places to hide if we provide accurate, verifiable, timely information to the people charged with protecting us.*

*Fear of government abuse of information, like fear of terrorism, is understandable. But we cannot let it stop us from doing what is right and responsible. The antidote to this fear, I might add, is an open, fair, and transparent process that guarantees the protection and privacy of that data.*

*In addition to the federal privacy safeguards already on the books, the Department of Homeland Security will have its own privacy officer. . . . That individual will be involved from the very beginning with every policy initiative and every program initiative that we consider, to ensure that our strategy and our actions are consistent with the individual rights and civil liberties protected by the Constitution.*

*We'll work together to ensure that our programs appropriately use information, protect it from misuse, and discard it when it is of no further use. It is, however, critical that information be accurate, comprehensive and up-to-date."*



Tom Ridge  
Secretary  
U.S. Department of Homeland Security



*"Privacy is a value that must be embedded in the very culture and structure of the organization. I know that we can and will succeed in this – because our leadership and our employees believe in and act on this value – for themselves, their neighbors, and their families – each day."*

Nuala O'Connor Kelly  
Chief Privacy Officer  
U.S. Department of Homeland Security

## TABLE OF CONTENTS

Privacy Office Structure.....	1
Key Privacy Frameworks.....	6
Privacy Policy Development.....	8
Privacy and Technology .....	15
Privacy Act Compliance.....	19
Legislative and Regulatory Reviews.....	22
Privacy Impact Assessments.....	24
Privacy Complaints.....	26
Internal Education; External Outreach.....	29
Departmental Disclosure Program.....	31
Implementing Privacy Oversight .....	33
The Way Forward: A Personal Note from the Chief Privacy Officer.....	38

## APPENDICES

Appendix A... Homeland Security Act, Sec. 222 PRIVACY OFFICER	
Appendix B... Privacy Office Mission Statement	
Appendix C... Privacy Office Biographies	
Appendix D... Keynote Address by Nuala O'Connor Kelly Before the 25 <sup>th</sup> International Conference of Data Protection and Privacy Commissioners, September 11, 2003	
Appendix E... Written Testimony of Nuala O'Connor Kelly Before the Committee on the Judiciary Subcommittee on Commercial and Administrative Law, February 10, 2004	
Appendix F... US-VISIT Program, Increment 1, Privacy Impact Assessment	
Appendix G... Systems of Records Notice for CAPPS II	
Appendix H... Report to the Public on Events Surrounding jetBlue Data Transfer	
Appendix I... Data Integrity, Privacy and Interoperability Advisory Committee Notice	
Appendix J... Freedom of Information Act Annual Report for FY 2003	
Appendix K... Privacy Office Outreach Highlights	

*For an online copy of this report, log on to [www.dhs.gov/privacy](http://www.dhs.gov/privacy).*

**THE DEPARTMENT OF HOMELAND SECURITY**  
**PRIVACY OFFICE**  
**REPORT TO CONGRESS**  
**APRIL 2003 - JUNE 2004**

**PRIVACY OFFICE STRUCTURE**

**Establishment of the Privacy Office**

The DHS Privacy Office is the first statutorily required comprehensive privacy operation at any federal agency. It operates under the direction of the Chief Privacy Officer, who is appointed by the Secretary. The DHS Privacy Office serves as the steward of Section 222 of the Homeland Security Act of 2002, and has programmatic responsibilities for the Privacy Act of 1974, the Freedom of Information Act, the E-Government Act of 2002, and the numerous laws, Executive Orders, court decisions, and DHS policies that protect the collection, use, and disclosure of personal and Departmental information. The Privacy Office ensures that appropriate access to or withholding of information is consistent with these statutes as well as with the Vision, Mission, and Core Values of DHS.

**Privacy Protection is an Integral Part of the DHS Security Mission**

Contributing to all of the Department of Homeland Security's Strategic Goals, the Privacy Office implements the Guiding Principles of the Department to defend and protect the individual rights, liberties, and the information interests of our citizens, residents and visitors. Secretary Ridge, in anticipation of his appointment of Chief Privacy Officer Nuala O'Connor Kelly, announced his vision of the mission of the Privacy Office, explaining that the Privacy Office "will be involved from the very beginning with every policy initiative and every program initiative that we consider," to ensure that our strategy and our actions are consistent with not only the federal privacy safeguards already on the books, but also "with the individual rights and civil liberties protected by the Constitution."

**Specific Privacy Office Responsibilities**

The Privacy Office has oversight of privacy policy matters and information disclosure policy, including compliance with the Privacy Act of 1974, the Freedom of Information Act, and the completion of Privacy Impact Assessments on all new programs, as required by the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002. The Privacy Office also is statutorily required to evaluate all new technologies used by the Department for their impact on personal privacy. Further, the Privacy Office is required to report to Congress on these matters, as well as on complaints about possible privacy violations.

## **Statutory Duties of the Chief Privacy Officer**

The responsibilities of the Chief Privacy Officer of the Department of Homeland Security as set forth in Section 222 of the Homeland Security Act of 2002, are to assume primary responsibility for privacy policy, including –

- (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information;
- (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- (3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
- (4) conducting a privacy impact assessment of proposed rules of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and
- (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.

*The Homeland Security Act of 2002*, Pub. L. No.107-296, Title II, § 222, 116 Stat. 2155.

## **Additional Responsibilities**

The work of the Privacy Office includes not only the statutory privacy work required under U.S. law, but also Freedom of Information Act (FOIA) compliance for the Department. This additional responsibility for FOIA compliance was delegated to the Privacy Office by the Secretary during the summer of 2003, in recognition of the close connection between privacy and disclosure laws, and the functional synergies of the work of more than 430 Privacy Act and FOIA specialists across the Department. Those specialists now work on Privacy Act and FOIA compliance matters under policy guidance from the Chief Privacy Officer.

Since the Department's focus is necessarily international as well as domestic, the Privacy Office addresses cross-border privacy issues. Compliance responsibilities of the Privacy Office include oversight of implementation of international arrangements that facilitate DHS program goals. Additionally, the Privacy Office is responsible for privacy-related education and training initiatives for DHS's more than 180,000 employees and new hires.

## **DHS Privacy Staff**

The Privacy Office's initial staffing at DHS headquarters has been recruited to functionally address major DHS privacy and transparency responsibilities as follows:

- Chief Privacy Officer;
- Chief of Staff and Director, International Privacy Policy;
- Chief Counsel for the Privacy Office (Office of the General Counsel);
- Director, Departmental Disclosure and FOIA;
- Director, Privacy Technology; and
- Director, Privacy Compliance.

Additionally, more than 430 Privacy and FOIA specialists throughout the Department contribute to compliance efforts and implement DHS privacy and FOIA policy each day.

Finally, three Privacy Officers, with dual reporting relationships to the Chief Privacy Officer and to their offices, have been appointed to the following areas: the US-VISIT Program, the National Cyber Security Division (within the Information Analysis and Infrastructure Protection Directorate) and the Transportation Security Administration (TSA).

### **Privacy Office Headquarters Staff Responsibilities**

*Chief Privacy Officer.* The Chief Privacy Officer (CPO) is responsible for policy oversight and implementation of the Privacy Act and FOIA, for office direction and policy creation, and for initiating and directing inquiries and investigations in cases of alleged privacy violations or misuse of personal information.

*Chief of Staff and Director, International Privacy Policy.* The Chief of Staff and Director, International Privacy Policy, coordinates implementation of policy direction and office management under the CPO and serves as senior advisor to the Department on international privacy frameworks and policies, advises on negotiations and external relationships with the European Union and other global regions, and handles international privacy matters and inquiries.

*Chief Counsel for the Privacy Office.* The Chief Counsel provides legal advice on the full range of issues concerning information disclosure and privacy law and reviews Privacy Office documents for legal sufficiency and statutory compliance. Embedded within the Privacy Office, the Chief Counsel is part of the DHS Office of the General Counsel, and reports to the Division of General Law.

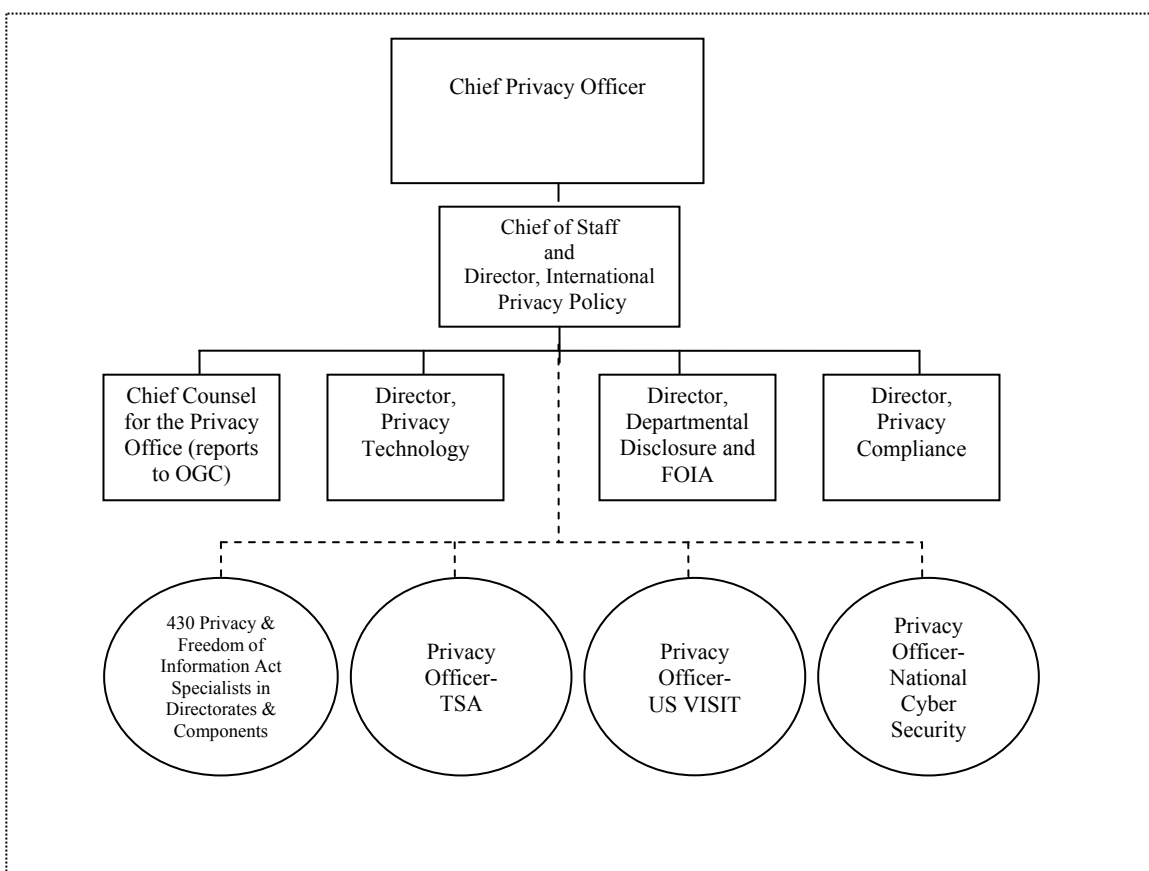
*Director, Departmental Disclosure.* The Director, Departmental Disclosure, oversees FOIA and Privacy Act disclosure compliance across the Department and directs Privacy Act and FOIA disclosure policy and is charged with creating a Privacy Act/FOIA appeals function at DHS headquarters.



*Director, Privacy Technology.* The Director, Privacy Technology, advises Departmental leaders on privacy-sensitive technology development, evaluates new technologies for privacy impact, enforces privacy policies on DHS websites and other citizen-facing communications, and serves as a liaison to the Chief Information Officer's Office, the Directorate for Information Analysis and Infrastructure Protection, and the Directorate of Science and Technology, in particular.

*Director, Privacy Compliance.* The Director, Privacy Compliance, assures compliance with privacy policy including privacy impact assessment requirements, by benchmarking the various components' privacy education and training, protocols, and protections, educates employees and leaders on best practices, and performs an internal audits function on privacy compliance.

### DHS Privacy Office Organizational Chart 2004



*Note:* In FY 2004, the DHS Privacy Office has been staffed with the direct reports shown above, as well as a number of contractors performing administrative operational functions and supporting the Privacy Act/FOIA function, as well as several short-term detailees from other directorates who serially provided FOIA support. We also have relied upon a number of detailees from other Federal agencies, including the Departments of Justice, Agriculture, and Commerce, for additional privacy program support.

## **Summary**

This Report on Department of Homeland Security privacy activities, covering the period from the creation of the Privacy Office until July 2004, demonstrates that, through the establishment and functionality of the operations of the DHS Privacy Office, we are working to “operationalize” privacy awareness and best practices throughout DHS.

We have made privacy an integral part of DHS operations by working side-by-side on DHS initiatives with the senior policy leadership of the various directorates and components of DHS and with program staff across the Department. As a result, the Privacy Office has been able to embed privacy values into the culture and structure of DHS in order to ensure that, as DHS programs move forward to implementation, they have been carefully and thoroughly analyzed for their impact on personal privacy and, once implemented, are effective in protecting the homeland while protecting personal privacy.

The DHS Privacy Office is pleased to share with Congress and the American people the policy and legal architecture applicable to DHS to safeguard individual privacy. This report contains the Privacy Office's milestones during the past fourteen months toward satisfying the objectives of those laws and the development of DHS privacy policy, pursuant to Section 222 of the Homeland Security Act of 2002.

## **KEY PRIVACY FRAMEWORKS**

### **The Privacy Act of 1974**

One of the primary laws supporting the mission of the DHS Privacy Office is the Privacy Act of 1974. The Privacy Act, 5 U.S.C. § 552a, provides a code of fair information practices that governs the collection, maintenance, use, and dissemination of personal information by federal agencies. Emanating from concerns about the ability to aggregate personal information -- due, in part, to advances in technology -- this law provides substantial notice, access, and redress rights for citizens and legal permanent residents of the United States whose information is held by the executive branch of the federal government. The law provides robust advance notice, through detailed "system of records" notices, about the creation of new technological or other systems containing personal information and carefully prescribed limits on the release of that information. The law also provides the right of access to one's own records, the right to know other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy or disclosure of those records. The Privacy Act is our country's articulation of Fair Information Principles; the Act both protects the information of our citizens and also provides our citizens rights to access that data.

### **Freedom of Information Act**

The Freedom of Information Act, 5 U.S.C. § 552, embodies the principle that persons have a fundamental right to know what their government is doing. Our government and our agency are grounded on principles of openness and accountability, tempered, of course, by the need to preserve the confidentiality of sensitive personal, commercial, and governmental information. The Freedom of Information Act is the primary statute that attempts to balance these countervailing public concerns. A robust FOIA/PA program is a critical part of any agency's fundamental processes; it helps to provide assurance to the public that, in pursuing its mission, an agency will also pursue balanced policies of transparency and accountability while preserving personal privacy. The federal government will spend hundreds of millions of dollars processing and responding to FOIA requests next year, and thousands of federal workers will spend all or part of their day compiling responses to those requests. Our agency alone has over 430 staff members across the Department who work full or part-time on FOIA and Privacy Act issues.

### **The E-Government Act of 2002**

Specific portions of the E-Government Act of 2002 are particularly relevant to the Privacy Office's function. Section 208 of the E-Government Act mandates Privacy Impact Assessments for all Federal agencies when there are new collections of, or new technologies applied to, personally identifiable information. In September 2003, the Office of Management and Budget released its guidance under Section 208. These requirements are further articulated in Section 222 of the Department's organic statute.

Privacy Impact Assessments, or PIAs, are a third pillar of the privacy framework at the federal level, and reflect the growing reliance on technology to move data -- both in government spaces and on the Internet. With the addition of the privacy provisions of the E-Government Act to existing privacy protections, individuals now benefit from a comprehensive framework within which government considers privacy in the ordinary course of business.

The Act and underlying guidance synthesize numerous prior statements and guidance on privacy practices and notices, and will assist privacy practitioners in prioritizing their efforts. In particular, the guidance provides direction on the content of privacy policies and on the machine-readability of privacy policies.

The Act and guidance outline the parameters for privacy impact assessments. These new requirements formalize an important principle: that data collection by the government should be scrutinized for its impact on the privacy of individuals . . . before that data collection is ever implemented. The process, the very exercise of such scrutiny, is a crucial step towards narrowly tailoring and focusing data collection towards the core missions of government. This practice should provide even greater awareness of the impact on the individual and the purpose of the collection, both by those seeking to collect the data and those whose data is collected. The Privacy Office is working with privacy practitioners across the agency, as well as with the Chief Information Officer (CIO), legal, and budget office teams to implement a rigorous PIA process, whereby every new technology use or acquisition is subject to a PIA.

### **A Unified Privacy Architecture for the Government Space**

Under the Privacy Act, in concert with FOIA and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them. A robust FOIA and Privacy Act program is imperative to provide the public with assurances that any information DHS collects is being maintained consistent with all requirements.

## **PRIVACY POLICY DEVELOPMENT**

*The Chief Privacy Officer of the Department of Homeland Security's responsibilities, as set forth in Section 222 of the Homeland Security Act, are "to assume primary responsibility for privacy policy. . .*

*Section 222,  
Homeland Security Act of 2002*

*"We at Homeland Security are forging a new way forward. This new way forward will require clear policies, definite policies, and intelligent choices about the responsible use of information by our government and by the private sector."*

*Nuala O'Connor Kelly  
Chief Privacy Officer  
October 30, 2003*

### **Pragmatic Optimism and Practical Privacy Objectives**

Pragmatic optimism has marked the approach to building privacy awareness and compliance into the culture, security mission, policies, practices and aspirations of the Department of Homeland Security. To that end, no one has been a greater supporter, in word and deed, than Secretary Tom Ridge. His active support for the independence of the Chief Privacy Officer and the establishment of a functioning Privacy Office, with a dedicated budget and strong input and influence on shaping DHS programs, has set the bar high for expectations of privacy compliance throughout the Department. Under Secretary Ridge and Deputy Secretary Jim Loy, the entire leadership team of the Department has embraced the value of privacy as an integral DHS cultural value and as an important sign of our respect for DHS employees, American citizens and legal permanent residents, and visitors to our welcoming nation.

In building privacy awareness into the fabric of DHS, three key challenges were identified in this initial year: (1) operationalizing privacy throughout DHS; (2) the need to address use of private sector data; and (3) international cooperation.

### **Operationalizing Privacy throughout the Department of Homeland Security**

In the first year of the Privacy Office, much time was given to what has been described internationally as "practical privacy." With the merger of 22 existing agencies to form a unified DHS, time was necessarily spent assessing current privacy and government transparency operations in the legacy component agencies and formulating a practical way forward for operationalizing privacy throughout the Department. The path chosen was to identify significant functional privacy areas and to assemble a seasoned team of privacy professionals to fill senior positions that addressed those functional objectives and to provide leadership at the Departmental level. To that end, as reflected in the earlier

portions of this Report, the Chief Privacy Officer determined the need for functional expertise to assist the Department with privacy technology, privacy compliance, privacy policy, disclosure policy and international privacy policy.

In operationalizing privacy, the Privacy Office reports directly to the Secretary and works collaboratively with senior policy leadership of the various agencies and directorates of the Department, as well as with more than 430 Privacy Act and FOIA team members, Privacy Officers, and other operational staff across the Department. Additionally, the DHS Privacy Office works collaboratively with Privacy Officers across the Administration and with privacy leaders at the Office of Management and Budget (OMB) and the Department of Justice, to consult on best practices and polices for agency privacy offices.

The Privacy Office works closely with the DHS General Counsel and the Chief Information Officer to ensure that the mission of the Privacy Office is reflected in all DHS initiatives. The especially close working relationship of the Privacy Office and the Office of the General Counsel, led by General Counsel Joe Whitley, enables DHS to meet its security mission, while protecting personal information by being fully counseled on the legal and regulatory ramifications of U.S. privacy laws and their interrelationship with statutes and proposed legislation affecting homeland security. And, of course, we also work in concert with the Department's Office for Civil Rights and Civil Liberties on matters of mutual interest and concern.

Much of this Report addresses operationalizing privacy in a new and changing organization. This is a challenging mission, and DHS is committed to complying with applicable privacy laws, best practices, and fair information principles. The Privacy Office has made significant progress in creating a strong foundation of privacy protections throughout DHS programs, technologies, and policies in our first year. We look forward to continuing the process of educating the more than 180,000 DHS employees on these matters.

One of the ongoing challenges that has persisted this year and will continue next year is everyday compliance with good privacy practices, including the need for privacy policies on DHS websites, the need to comply with all privacy laws. This compliance includes not just the Privacy, FOIA and E-Government Acts, but also the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and other pertinent laws, if they are applicable to DHS programs or information sharing, including concerning employee information. The need for education and training is made all that much more clear by these examples and other areas, such as the legal mandate for privacy impact assessments, to educate and remind our employees on compliance requirements and due care.

Also in this first year, in terms of emphasis and available staff resources, a great deal of Privacy Office review and assistance has been given to programs emerging from the Directorate of Border and Transportation Security (BTS), in particular, from the Transportation Security Administration and Customs and Border Protection components, to assist with the immediate mission of securing and facilitating travel and borders. Under Secretary Asa Hutchinson and Assistant Secretary Stewart Verdery have, in particular,

been active leaders and partners in making sure that BTS programs reflect the security and privacy protection objectives of the Department.

Approximately 120,000 of DHS's more than 180,000 employees work within the BTS Directorate. Their efforts are on the front line of developing programs and protocols for better securing our homeland from terrorists and others who seek to threaten the freedoms of our citizens and those who visit what is, and has always been, our welcoming nation. To that end, the Privacy Office played an integral advisory role concerning all phases of the US-VISIT program and proposed CAPPS II program. In response to operational factors and internal and public comments concerning CAPPS II, DHS has redesigned an automated advanced screening program and recently announced a new domestic program, Secure Flight. The Privacy Office has provided assistance and collaboration on many other border and transportation security programs, including those related to screening of hazardous materials drivers and registered travelers, to ensure that privacy considerations and protections for all individuals are built into DHS programs.

### **Use of Private Sector Data**

One of the most important public policy challenges facing not only DHS but also the federal government as a whole is the sharing of personal information between the public and private sector. This issue resonates with American citizens, foreign visitors, political leaders both at home and abroad, and within DHS where the responsible handling of personal information is critical to the successful performance of our mission.

The Privacy Office's examination of the events surrounding alleged privacy violations concerning voluntary transfers of passenger name record (PNR) data from the private sector to the government is one example of why it is so important to have in place all necessary protections for personally-identifiable information. Even when actual Privacy Act violations are not found, it is nevertheless important that clear rules be in place to ensure that information sharing is done in a legitimate, respectful, and limited way. Going forward, the challenge facing the Privacy Office is to carefully navigate between the privacy and security concerns inherent in information sharing and to build a consensus on the responsible use of private sector data so that we can further our efforts to enhance homeland security while maintaining robust protections for personal privacy.

To that end, the Privacy Office has been engaged in dialogues with many private sector groups, encouraging them to develop their own internal guidelines as well as recommendations for "best practices" for public-private data sharing so that the Privacy Office can obtain a range of views and input on this matter. The appropriate use of private sector information by DHS is also one of the major issues that the *Data Integrity, Privacy, and Interoperability Advisory Committee*, now being formed, will consider as a first order of business. That Committee will reflect the diverse viewpoints of all sectors -- business, academia, privacy advocacy, technology and security specialists, and policy generalists. (See Appendix I)

A related topic discussed further below is "data mining." Technology has broadened exponentially our ability to extract information from data. It is important that we bring fair information principles to the quest for knowledge from existing and new data

sources in order to legitimize our efforts and build a consensus on respectful use of the information that is available to us.

Through the issuance of public reports, the Privacy Office has and will continue to share with Congress and the public information regarding investigations and conclusions about data sharing and data mining.

## **International Cooperation**

Since the Department's work affects not only citizens but also visitors to our country and persons throughout the world, the Privacy Office's work is necessarily international as well as domestic. A key focus of the Privacy Office's work in this first year has been to engage data protection authorities and privacy and security advocates internationally. In these efforts, of course, we ensure interagency policy coordination.

### *Outreach*

Significant efforts have been spent on outreach by the Chief Privacy Officer and the Chief of Staff and Director for International Privacy Policy. The Privacy Office has met with Data Protection and Privacy officials from Canada, the European Union, Australia, Asia, and Latin America in 2003-2004. The Chief Privacy Officer has testified before a committee of the European Parliament and was a speaker before the International Association of Data Protection and Privacy Commissioners in 2003. In all cases, the purposes of these interactions have been, in part, to better explain the privacy framework that exists in the United States, which protects the privacy of personal information when it is collected, used, shared and retained by the U.S. government.

Our dialogues have resulted in the beginnings of greater understanding of the U.S. system, but have also revealed a nearly universal misconception that the United States has no privacy framework that might be viewed as consonant with those of other countries. In fact, this is not the case, particularly with respect to privacy laws applicable to the public, governmental sphere – the Privacy Act of 1974 that has been in existence and use for 30 years that provides access and redress rights to all individuals with respect to their own personal information, and the Freedom of Information Act that provides access to government records including personal information, and the E-Government Act of 2002 that requires Privacy Impact Assessments of all new technologies and government databases that collect or store personal information about any individual, whether a U.S. citizen or not. (See above, *Key Frameworks Enforced by the Privacy Office*)

The fact that our most basic and overarching implementation of fair information principles is embodied in the Privacy Act of 1974 and, according to a plain reading of the statutory language, protects only the privacy interests of U.S. citizens and permanent residents whose information is collected by the U.S. government, has presented a challenge in our international dialogues. Global neighbors communicated their perception that the U.S. interest in privacy protection and privacy rights may be parochial, isolated to Americans only, fueling the misperception of U.S. non-comparability with basic information privacy protections afforded in many other regions of the world to any individual, regardless of status. Arguably, this was one of the most serious points of



discussion and concern from the European side during the recently concluded negotiations on permitting the sharing of Passenger Name Records with DHS's Customs and Border Protection component to assist in advance passenger screening of travelers flying between the U.S. and the European Union.

### *Common Dialogue with Shared Privacy Principles*

Privacy professionals and officials the world over, share a common interest in assuring public trust in government operations by encouraging government transparency, as well as respect for fair information principles in handling personal information, such as collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, participation and accountability. Sometimes these concepts are articulated using different titles, but the notions remain substantially similar. An important bridge in communications across borders, where legal systems may differ significantly and, thus, also the presentation of privacy protections, are common understandings about guidance provided by voluntary, internationally recognized privacy principles.

To that end, the Organization for Economic Cooperation and Development's (OECD's) Privacy Principles, long standing since the early 1980s (shaped, in part, by the fair information principles of the U.S. Privacy Act of 1974), and the emerging principles from the Asia-Pacific Economic Cooperation (APEC) concerning data handling in a networked world, all are important in promoting cross-border cooperation. They provide the vehicles and needed flexibility for recognizing the privacy protections of different economies and regions that reflect differences in culture, political structures and legal systems, but share a common foundation grounded on accepted privacy principles. To this end, DHS participation in multilateral groups that consider international privacy principles and their applications is critical in developing working relationships and international cooperation on a variety of homeland security measures.

One example of the potential for employing international privacy principles as a bridge in dialogues among global neighbors and security partners has been in the context of joint work by the International Civil Aviation Organization (ICAO) and the OECD's Working Group on Information Security and Privacy (WPISP). The effort centers on developing an international information-sharing system that will facilitate real-time sharing of data on lost or stolen passports. Use of fraudulent or lost and stolen passports by terrorists and by serious transnational criminals threatens the security of America and our global neighbors. The United States, and DHS, in particular, supports this joint work of ICAO and the OECD, which promotes the use of OECD Privacy Principles as a framework for dialogue and policy guidance from the OECD-WPISP on how to design the information-sharing system's architecture to include privacy enhancing protections while effectively achieving needed homeland security controls. The Privacy Office's Chief of Staff and Director of International Privacy Policy has been the U.S. Delegation spokesperson at the OECD WPISP on this initiative, supporting U.S. efforts in many multilateral settings and in bilateral relationships for Enhanced International Travel Security programs.

Additional areas where dialogues center on accepted international privacy principles, rather than on legal differences of countries, include the use of biometrics and

new technologies in an array of homeland security enhancing programs and applications. These include dialogues within the International Standards Organization, the OECD, and ICAO, among other multilateral venues.

### *Engaging Data Protection Authorities Internationally*

An important focus of the Privacy Office's work has been to engage the data protection authorities internationally. Our office has participated in meetings of the International Data Protection and Privacy Commissioners, although our office is not recognized at this time as an accredited data protection authority.

The Privacy Office has, however, submitted an application for and been approved as an official "Observer" to the International Data Protection and Privacy Commissioners Conference, in order to participate in both open and closed discussions among governmental data protection authorities from around the world on the serious issues relevant to protecting individual privacy. Today, these issues often focus on information privacy and the use of emerging technologies in a networked world for homeland security and other data sharing purposes.

The acceptance of this application represents the first official U.S. government representation within this body, notwithstanding wide participation from countries from every region in the world. We believe it is in the interest of the American people we serve, and would assist us in addressing concerns of visitors and building bonds with global neighbors, to be at the table as listeners, learners, participants, partners and advocates. We are confident that the important dialogues within this body will increase opportunities for international cooperation and will demonstrate a unified commitment world-wide to protecting individual freedoms.

### *Other International Privacy Issues*

The Privacy Office has actively engaged in international discussions and participated in domestic and international workshops on the design of effective Privacy Notices, including short-layered privacy notices. These discussions broadly involved data protection authorities, consumer and privacy advocates, and multinational businesses representatives from the United States, Europe, and Australia.

In addition to domestic discussions on the use of technologies in a privacy enhancing, rather than an intrusive, manner, the Privacy Office has participated in discussions on a range of technology issues with other data protection staff and privacy advocates from Europe and Latin America and the United States through the International Working Group on Data Protection in Telecommunications. These discussions span technologies such as RFIDs to biometrics and many other issue areas.

Other issues that come up in the context of international privacy issues internally for review and in the context of international outreach include G-8 proposals that include a recognition of the need for privacy reviews in the design and implementation of the proposals, issues concerning maintaining data integrity and, generally, the protection of personal information in a cross-border context.

## *Compliance*

Compliance responsibilities of the Privacy Office include oversight of implementation of international arrangements that facilitate DHS program goals. These currently include the recently concluded U.S.-EU PNR Agreement and the US-EU Europol Agreement on Data Protection.

The Privacy Office played a significant role within DHS during the US-EU PNR Agreement negotiations, by providing advice on fair information practices, and European Data Protection law and its implementation. In connection with those negotiations, the Chief Privacy Officer and the Director for International Privacy Policy traveled with the U.S. team to facilitate dialogues and information exchanges about U.S. privacy practices with European Commission members and staff, members of the European Parliament, U.S. Embassy staff in Europe doing outreach from their posts, advocacy groups and foreign press.

Since the PNR Agreement was signed in May 2004, the Privacy Office has proactively assisted with implementation efforts, including posting a Privacy Statement concerning the Agreement on its website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), composing Frequently Asked Questions for further notice to the public and suggested privacy statements that might be used by airlines, travel industry representatives, and central reservation systems. Internally, the Privacy Office has a role in auditing compliance with the terms of the Agreement and Undertakings. The Privacy Office will facilitate the annual joint review of progress made on implementing the PNR Agreement and Undertaking representations.

Under the terms of the Undertakings, as a result of concerns expressed about non-citizens or non-residents not having the same privacy protections for information collected by the U.S. Government that are extended under the Privacy Act to Americans citizens and permanent residents, the Privacy Office itself will function as a clearinghouse for international correspondence or complaints related to the PNR Agreement, and will provide a special appeals function, as well, at the Departmental level for complaints and questions. A foreign national may contact Customs and Border Protection and the Privacy Office directly or through their member country data protection commissioner and priority review will be given to such complaints/contacts. While this feature is specific to the U.S. – EU PNR Agreement, within the Privacy Office we look forward to working with Data Protection Authorities from any region in assisting them help their citizens or residents pursue reviews in connection with privacy concerns or possible privacy violations related to DHS activities.

## PRIVACY AND TECHNOLOGY

*“ . . . (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection and disclosure of personal information;”*

*Section 222 (1), The Homeland Security Act of 2002*

The Department constantly seeks to leverage the newest technology tools in the War on Terrorism. New data technologies can support new ways of looking at existing information and can offer new opportunities for collecting and analyzing information. When so many of these data collections impact personal information, privacy protections are an essential element of such technological tools. As a result, ensuring that privacy is part of the core architecture of new technologies is one of the key missions of the DHS Privacy Office.

In fact, the very first task for the DHS Privacy Officer enumerated in Section 222 of the Homeland Security Act of 2002 is to “assure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information.” As a result of this mandate, the Privacy Office has been involved from the very beginning in numerous DHS initiatives that apply technology to the collection of personally identifiable data.

A primary goal of the Privacy Office is to raise the level of privacy awareness and develop active communications among scientists, engineers, and other technicians who are investigating options and crafting proposals for DHS's technological response to terrorism. The Privacy Office has accomplished this by working with the science and technical organizations across the Department as well as with the private sector.

By examining technologies generally, independent of any particular application within the Department, the DHS Privacy Office is able to bring a privacy framework to the Department for major areas of technology that can be used Department-wide. This “outside look” at specific technologies also streamlines the process of ensuring that as various organizations approach the same technology across different applications, the issues that are raised by that common technology are addressed from a single perspective. In consequence, the Privacy Office can ensure that technology is consistently implemented and structured to account for issues of privacy protection and awareness.

The following are some specific technologies that the DHS Privacy Office has actively examined:

### **Biometrics**

One tool that appears increasingly promising for use in securing the homeland is biometrics. Biometrics refers to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition. The Department is leading the way in exploring the use

of these technologies for identification purposes, and the Privacy Office has ensured its place at the table so that privacy concerns can be addressed at all points along the development and implementation phases.

One of the primary programs collecting and using biometrics is the US-VISIT Program. The Chief Privacy Officer is a permanent member of the oversight board for the US-VISIT Program and reviewed and assisted in “baking in” privacy protections to the architecture of the program. The US-VISIT program is discussed further at Part 5 of this Report. (See also the US-VISIT Privacy Impact Assessment at Appendix F.)

From its inception, the DHS Privacy Office has been an active participant in a series of different biometrics committees and working groups at various levels of government and industry.

#### *Biometrics Coordination Group*

The DHS Privacy Office has been actively engaged in the “Biometrics Coordination Group” within the Department, which ensures that all biometrics work across all of DHS approaches the technology from a harmonized perspective and with awareness of each individual application of the technology.

#### *National Science & Technology Council’s Inter-Agency Working Group on Biometrics*

The DHS Privacy Office is co-chair of the Social/Legal/Privacy subgroup of this Inter-Agency working group. In that role the Privacy Office is actively influencing governmental implementation of biometric technologies from a privacy protection perspective.

#### *Biometrics Interoperability and Programs*

The DHS Privacy Office is an active member of this interagency program to identify opportunities for focusing expertise from multiple agencies to benefit biometrics programs on a government-wide basis.

#### *International Working Groups*

Through its participation in groups such as INCITS (The International Committee for Information Technology Standards), ISO (The International Organization for Standardization), ICAO, the OECD’s Working Party on Information Security and Privacy and other multilateral groups, the DHS Privacy Office is actively engaged internationally in the discussion of how biometric technologies and privacy protection considerations can best fit together. This is true particularly in the context of information sharing on lost and stolen passports and other programs for enhanced international travel security, including the development of machine readable passports that contain biometric identifiers.

## **Radio Frequency Identification Devices**

RFID (Radio Frequency Identification Devices) are another technology series drawing significant attention from the Privacy Office. RFIDs have been defined as “an analog-to-digital conversion technology that uses radio frequency waves to transfer data between a moveable item and a reader to identify, track or locate that item.”<sup>1</sup> The DHS Privacy Office has been actively engaged in many discussions regarding the use of RFID technologies across both government agencies and industry.

In the period covered by this report, the DHS Privacy Office participated in the Federal Trade Commission’s workshop on RFID technology and also in a working group of the Center for Strategic and International Studies. Both of these events brought together members of federal government agencies, academicians, industry users, and researchers to examine how the technology operates and the related privacy and policy implications. As a result of these discussions, should RFIDs be proposed for use in connection with DHS programs, the Privacy Office will be better able to ensure that the technology is used in ways that enhance rather than erode privacy protections.

Internally, the Privacy Office has reviewed proposals for possible use of RFID technologies, including a piloted program at two airports to track baggage through the security process. The pilots tracked the movement of “things” rather than “people,” in order to better enhance travel by making sure that the luggage of travelers reaches the correct airliner once any security check has been completed.

## **“Data Mining”**

The term “data mining” has many connotations, not all of which are positive. One of the major goals of the Privacy Office is not only to build a consensus for arriving at a common meaning for this term within DHS, but also, more importantly, to arrive at a consensus on an appropriate policy for using databases – both public and private – to enhance the knowledge of personnel across DHS who are actively engaged in the War on Terrorism and serious crimes threatening the homeland, particularly in protecting our borders, ports and major infrastructures.

The Privacy Office has been engaged in this effort on a practical level. One definition of data mining recognizes the concept of “distributed data environments” – where data stays with the “owner,” but queries are performed across the network where the data is stored. With the DHS Directorate of Science and Technology (S&T), the Privacy Office participated in a workshop concerning “distributed data environments,” which also drew in representatives from the San Diego Supercomputer Center, from the private sector and from academic institutions. The focus of these and other discussions with DHS staff and academicians is to foster mutual understanding of privacy protection principles and strategies for those who are researching and developing distributed technology. The DHS

Privacy Office is also working with S&T on using distributed system architecture to enhance travel and travel document security from a privacy-centric perspective.

In this area, the Privacy Office has also taken specific steps to ensure that data mining programs that receive DHS funds conduct their activities with the utmost concern for personal privacy, and that they employ best practices regarding their use of personally identifiable information. To that end, the Privacy Office has undertaken a comprehensive review of the Multi-State Antiterrorist Information Exchange (MATRIX), a network of law enforcement databases that has received some DHS support through a cooperative agreement.

In the near future, the Privacy Office will issue a report assessing the benefits and deficiencies of MATRIX and the role of DHS in supporting the program. That report, like all of the activities of the Privacy Office, is motivated by the belief that building a privacy architecture on the front-end for technology-driven programs is the best way to ensure that preventable instances of error and abuse do not hinder important efforts at all levels of government to share information and prevent terrorist attacks.

### **“New” Technologies**

Information technologies are regularly pushed to their limits, stretched and combined to create new technologies and new uses of existing technologies. Many of these new technologies are not easily categorized and thus do not fit easily into existing privacy protection assessments. To the extent that DHS offices have explored such “new” technologies for potential applications, the DHS Privacy Office has ensured that the privacy protection issues are part of any preliminary discussions. Sometimes these discussions take place informally – in discussions among colleagues. At other times, the discussions are much more formal – occurring at workshops and conferences.

In addition to collaboration with DHS offices, the DHS Privacy Office also looks ahead at emerging technologies that may raise privacy protection concerns in the future. This separate research initiative focuses on broad issue-spotting and general preparedness for areas in which privacy and technology may merge to create new challenges to integrating privacy protections with new technology that may be used to further secure the homeland. Some examples of these new “new technologies” are geospatial information systems and services, unmanned aerial technologies and ubiquitous sensor networks. Each of these “forward-edge” technologies, among others, may potentially raise separate privacy protection concerns and, to that extent, the Privacy Office is taking the lead for DHS in reviewing their proposed or hypothetical uses and their impact on individual privacy, actively commenting within DHS and as part of larger discussion groups across the U.S. government on next generation information technologies.

In addition to addressing the privacy protection issues raised by today’s technology, the DHS Privacy Office serves DHS offices by scouting issues raised by potential technologies of the future so that if and when those “next” technologies are

---

<sup>1</sup> [http://www.cnet.com/video/webcast/wireless\\_glossary.html](http://www.cnet.com/video/webcast/wireless_glossary.html)

brought to the Department of Homeland Security, the framework of privacy protections can be addressed up front, rather than after research efforts and expenses are expended.

Regardless of the format, however, the Privacy Office has pursued its mission to ensure that an appreciation of privacy requirements is part of the developmental life cycle of any program, system, or use of technology.

## **PRIVACY ACT COMPLIANCE**

*“ . . . (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;”*

*Section 222 (2),  
The Homeland Security Act of 2002*

*The purpose of [the Privacy Act] is to promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals.*

*Senate Report 93-1183,  
September 26, 1974*

In accordance with Section 222 of the Homeland Security Act of 2002, the Privacy Office ensures that DHS activities comply with the Privacy Act of 1974. Specifically, the Privacy Act requires government agencies to publish notices in the Federal Register upon the establishment or revision of systems of records, to account for disclosures of certain records, and to agree in writing with another agency before entering into a computer matching program,<sup>2</sup> and to provide individuals access to records maintained about them.

### **Systems of Records**

#### *Legacy Systems of Records*

The Privacy Office is engaged in taking inventory of all Privacy Act systems of records in order to reorganize and republish them under the DHS umbrella. This is a significant undertaking; close to 200 systems of records have been identified across DHS and its 22 component agencies that pre-existed the creation of the Department of Homeland Security. In the process, the Privacy Office will reorganize and streamline its



systems of records, ensure that the routine uses<sup>3</sup> are consistent and appropriate across the agency, and that each office systematically has procedures in place accounting for data sharing.

#### *New Systems of Records Notices*

By the end of December 2003, DHS Headquarters and components had published eight new Privacy Act notices in Volume 68 of the Federal Register at the following cites: 68 Fed. Reg. 45265-01; 68 Fed. Reg. 49496-01; 68 Fed. Reg. 55642-01; and 68 Fed. Reg. 69412-01 and 69414-01.

New notices included an interim final notice for the CAPPS II Program<sup>4</sup> and a notice about a new system of records for SAFETY Act information collected by the Department. They also included republication of three notices by the Transportation Security Administration within DHS and two from the Directorate for Border and Transportation Security which were revised to accommodate the inauguration of the US-VISIT Program on December 12, 2003. Additionally, the Coast Guard announced its Health Information Privacy Program on April 28, 2003, which allows for appropriate uses and disclosures of protected health information concerning members of the Armed Forces.

Many other Privacy Act notices are now being drafted or revised and will be thoroughly reviewed by the Privacy Office to ensure compliance with the Privacy Act, as well as with fair information principles, generally, for the collection of personally-identifiable data.

#### *Accounting for Disclosures*

DHS components have in place memoranda of understanding allowing for the regular exchange of law enforcement data with federal and state agencies, such as through the Treasury Enforcement Communications System, as well as routine uses that permit release of Privacy Act data under carefully controlled circumstances to appropriate foreign, federal, state and local agencies. The DHS Privacy Office worked to ensure that all DHS employees remain cognizant of the need to account for any Privacy Act disclosure of records and to promote the use of technology in new record systems to facilitate these accountings in ways that are privacy enhancing.

#### *Matching Agreements*

U.S. Citizenship and Immigration Services (CIS) and the Coast Guard have matching agreements. CIS matching agreements involve the SAVE Program, Systematic Alien Verification for Entitlements Program, and facilitate the exchange of information between California, Colorado, New York, New Jersey, the District of Columbia,

---

<sup>2</sup> A “matching program” is a computerized comparison of two or more automated systems of records for the purpose of determining eligibility for a payment under a Federal benefit program or recouping payments already made.

<sup>3</sup> Under the Privacy Act, a “routine use” is the use of a record that is compatible with the purpose for which the record was collected.

<sup>4</sup> The CAPPS II Program has since been replaced by a new program, Secure Flight.

Massachusetts and the Department of Education to verify alien applicant eligibility for Supplemental Security Income, Temporary Assistance for Needy Families, food stamps, Medicaid, unemployment and, in the case of the Department of Education, educational assistance. The Chief Privacy Officer approved a one-year renewal of several matching agreements with the states concerning Social Security and welfare benefits during 2003.

The Coast Guard participates in two matching agreements with the Department of Defense, the Veterans Administration and the Social Security Administration to verify eligibility for supplemental security income payments and special veterans' benefits. These agreements were initiated prior to the establishment of the Department of Homeland Security and are eligible for renewal in 2004.

### *Requests*

Although Privacy Act requests for access to information or redress typically are included in agencies' annual FOIA reports and not separately reported, some DHS components have the capability separately to identify these requests. Based on reports from its components, DHS closed approximately 24,000 Privacy Act requests during fiscal year 2003. The vast majority of these requests were processed by United States Citizenship and Immigration Services which maintains, among other systems of records, the Alien File and Central Index System, consisting of records concerning all persons who are subject to any provision of the Immigration and Nationality Act. These data help to demonstrate that privacy is a core value at the heart of DHS's mission.

## LEGISLATIVE AND REGULATORY REVIEWS

*“ . . . (3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;”*

*Section 222 (3), The Homeland Security Act of 2002*

The Chief Privacy Officer for DHS is required by statutory mandate to evaluate all legislative and regulatory proposals involving the collection, use and disclosure of personally-identifying information by DHS. Institutional processes within DHS have been established to ensure that this occurs in a systematic fashion.

### **Legislative Proposals**

The Privacy Office works closely with the DHS Office of Legislative Affairs and the Office of the General Counsel to ensure that all bills on which DHS is asked to record its opinion that in any way concern individual privacy matters, the collection of personal information, agency disclosure policies, information sharing with DHS partners, or matters likely to be of significant interest to the international privacy community are reviewed by the Privacy Office. On any typical day, in fact, it is not uncommon for the Privacy Office to provide comments on numerous legislative proposals.

### **Regulatory Initiative Reviews**

Similarly, the Privacy Office works closely with the Office of the General Counsel to ensure that all DHS regulatory initiatives are reviewed for compliance with federal privacy law and DHS policy. No notice of proposed rulemaking that affects the collection of personally identifiable data goes forward for Federal Register publication without concurrence by the Privacy Office. Moreover, the Privacy Office has instituted policies to ensure that Privacy Impact Assessments, which are required by the E-Government Act of 2002, are published in the Federal Register and are made available prior to or in connection with the publication of notices of proposed rulemaking that cover the applicable programs.

The influence of the Privacy Office on regulatory developments is illustrated by the regulatory history of the CAPPs II Program. While still a part of the Department of Transportation, the Transportation Security Administration proposed a new system of records under the Privacy Act for "Passenger and Aviation Security Screening Records" in January 2003, prior to the installation of the Chief Privacy Officer for DHS. After the Chief Privacy Officer assumed her responsibilities, however, the proposed system notice for these records was significantly and substantially revised, in large part due to the public comments received on the initial notice, and a new notice, including a request for additional public comments, was published on August 1, 2003. That notice indicated that a further Privacy Act notice would be published in advance of any active implementation of the CAPPs II system, a decision made at the direction of the DHS Privacy Office. (See Appendix G)

In 2004, the Department announced a new domestic automated passenger prescreening program, Secure Flight. The new program is designed to more accurately authenticate the identity of travelers and to screen appropriately for heightened risks for terrorism. The Privacy Office anticipates that going forward it will continue to exercise close oversight over the final parameters of Secure Flight to ensure that robust privacy protections are fully implemented in the system architecture.

### **Congressional Testimony**

On February 10, 2004, the Chief Privacy Officer testified before the Subcommittee on Commercial and Administrative Law of the Judiciary Committee of the U.S. House of Representatives regarding the activities of the Privacy Office. Ms. O'Connor Kelly outlined the Department of Homeland Security's commitment to privacy protection, the establishment of the Privacy Office, the key frameworks enforced by the Privacy Office, the challenge of operationalizing privacy throughout DHS through best practices and consistent policies and education efforts, public outreach, policy challenges, and the need to balance transparency and security operations. (See Appendix E) In addition to this testimony, the DHS Privacy Office frequently reviews the Congressional testimony of other DHS representatives to ensure consistency in DHS statements on the importance of privacy to the agency's mission.

## PRIVACY IMPACT ASSESSMENTS

*“ . . . (4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;”*

*Section 222 (4), The Homeland Security Act of 2002*

*“Privacy Impact Assessments are a new and important tool in the tool belt of privacy practitioners across the federal government.”*

*Nuala O’Connor Kelly, Chief Privacy Officer  
Speech to Heritage Foundation, November 17, 2003.*

In accordance with Section 208 of the E-Government Act of 2002, the Department of Homeland Security is required to issue Privacy Impact Assessments (PIAs) when the agency substantially modifies existing information technology systems or creates new information technology systems that contain personally identifiable information. The purpose of a PIA is to ensure that information technology systems of the Federal Government are maintained in conformity with fair information principles concerning notice, consent, access, redress, data integrity and security.

Separately, Section 222 of the Homeland Security Act of 2002 requires the Chief Privacy Officer for DHS to require and review PIAs for proposed rules of the agency.

A PIA must address at least two issues:

1. It must determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system.
2. It must evaluate the protections and alternative processes for handling information to mitigate potential privacy risks.

A PIA outlines salient points about new or existing information technology systems by answering questions about the information that will be collected, the opportunity individuals will have to redress information collected about themselves, who will be able to access the information, how the system and data will be maintained, what administrative controls will be in place, and how the decision to use a system was made.

The Privacy Office has been instrumental in making the PIA process a focal point for privacy activities at DHS. By providing written and oral training in addition to specific guidance materials, the Privacy Office has enabled all DHS program offices to incorporate privacy into their fundamental program planning.

The effective date of the PIA requirement roughly coincided with the establishment of the DHS Privacy Office. This confluence of events allowed the Chief Privacy Officer

the opportunity both to provide DHS input into the final OMB guidance and to ensure that the PIA process became firmly embedded in the Department of Homeland Security.

From the initial drafting of a PIA to the final product, the Privacy Office has provided PIA leadership to DHS offices and components. A Privacy Office publication, *PIAs Made Simple*, is in use throughout the agency, and several PIAs for major DHS initiatives have set the standard for agency documents of this kind.

In addition to PIA development for programs since April 2003, the Privacy Office has reviewed nearly 90 PIAs in connection with the OMB 300 process, which requires privacy impact assessments in connection with any funding request of more than \$500,000 for new technologies or improvements on existing information systems and technologies. Additionally, the Privacy Office is reviewing PIAs, or advising on the need for their development, in connection with DHS rulemakings. Finally, as a policy matter, the Privacy Office may request that a DHS office or component undertake the preparation of a PIA to assist with a privacy review of a non-IT or rule-based proposal for a DHS program.

The Chief Privacy Officer provides final agency review of PIAs before they are forwarded to the Office of Management and Budget and then published in the Federal Register, or otherwise made publicly available. The Privacy Office has provided critical privacy advice to new DHS initiatives, resulting in changes in many cases that will improve privacy protections in DHS programs. Procedures are now well established to ensure that privacy is considered throughout the lifecycle of DHS processes and programs and that fair information principles inform policy decisions concerning data collection and use.

## PRIVACY COMPLAINTS

*“ . . . (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.”*

*Section 222(5), The Homeland Security Act of 2002*

The Privacy Office has examined privacy practices at the Department in a variety of ways, including through the lens of complaints. This review has encompassed alleged systemic violations of privacy and more particular violations concerning particular individuals.

### **JetBlue Data Transfer**

An alleged privacy violation involving the Transportation Security Administration was brought to the attention of the Privacy Office in September 2003. The potential violation involved the transfer of Passenger Name Records (PNRs) from JetBlue Airways to the Department of Defense, a transfer that was facilitated by certain personnel of the Transportation Security Administration. While the time of the potential violation predated the creation of the Department of Homeland Security, the matter raised serious concerns about the proper handling of personally identifiable information by government employees now within DHS.

In addressing the potential privacy violation, the Privacy Office thoroughly analyzed the matter, ultimately deciding that a Privacy Act violation had not occurred. The Privacy Officer found, nevertheless, that prophylactic action was required. Consequently, the Privacy Office made several recommendations regarding the need for privacy training for TSA employees as well as for DHS employees generally, the need to establish guidelines for data sharing, the need to have in place stronger controls for private-sector data sharing and the need to have the Inspector General review the matter to determine if further IG action is required. The Privacy Office report on the transfer of JetBlue PNR data is available to the public on the DHS website.

[http://www.dhs.gov/interweb/assetlibrary/PrivacyOffice\\_jetBlueFINAL.pdf](http://www.dhs.gov/interweb/assetlibrary/PrivacyOffice_jetBlueFINAL.pdf)

### **Other Airline Data Transfers**

Subsequent to the JetBlue report, the Privacy Office was alerted to the fact that additional PNR transfers had taken place with the involvement of TSA. Accordingly, the Privacy Office is now reviewing these additional transfers to ascertain if they were accomplished in compliance with applicable privacy laws and regulations. A further public report is anticipated as a result of this investigation.

## **Matrix**

Another example of the Privacy Office's investigatory efforts in response to privacy complaints involves the MATRIX program (Multi-State Anti-Terrorist Information Exchange), a system of integrated law enforcement and commercial databases that has been funded through a cooperative agreement with the DHS Office of Domestic Preparedness. From its inception, the system has been subjected to a substantial number of complaints and inquiries to the Privacy Office.

In response to these requests and ongoing concerns from various segments of the public, the Privacy Office has undertaken a full-scale review of the MATRIX program, seeking to gain an understanding of its components and functions and the role of the Department in supporting it. The results of that review will be made public in the near future through a forthcoming report.

## **CAPPS II**

From April 2003 until the present, the Privacy Office received thousands of contacts, most via e-mail and many in identical form, expressing concerns with respect to the proposed CAPPS II program. Much of the correspondence came in the form of public comment to privacy notices on the proposed program that were published in the Federal Register, seeking such comments. E-mail correspondence received automatic acknowledgements of receipt. The Chief Privacy Officer reviewed the contacts with the office and took the concerns expressed into consideration in formulating internal privacy guidance to program managers and DHS leadership. Additionally, the Chief Privacy Officer had numerous discussions with privacy advocates and other private sector representatives concerning the program's development about the need to address privacy concerns.

Many of the CAPPS II complaints centered on fears that the program would be a broad surveillance program that targeted innocent citizens and travelers, rather than narrowly tailored to potential terrorists. Other complaints expressed concern about the use of private sector data sharing with DHS in a manner that might lead to discriminatory treatment based on data, the integrity of which could not be verified and concerns that the data might not be covered by Privacy Act protections. Still others complained about lack of notice on the program details and what appeared to be a lack of robust access and redress rights for individuals.

## **International Privacy Complaints**

Fewer than a dozen pieces of correspondence were received by the Privacy Office at the Departmental level relating to international inquiries about DHS programs or information that DHS may have collected about an individual on travel to or through the United States. Most of the matters were requests for the an individual's personal information held by DHS, what exactly was collected in connection with airline flights, how was it used and for what period would such information be retained – whether Passenger Name Record information or Advance Passenger Information System (APIS) information. Included in these contacts were several letters from members of the European



Parliament, one from a European Data Protection Commissioner on behalf of a European citizen, one from a Canadian Data Protection Commissioner requesting information on the impact of the Patriot Act and privacy protections for Canadian personal data outsourced to a U.S. company, and several letters from individuals believing that they were on a No-Fly List or seeking confirmation that they were not. After reviewing the issues raised, the Privacy Office provided appropriate responses in each case.

## **INTERNAL EDUCATION; EXTERNAL OUTREACH**

*“The role of a privacy officer . . . is simultaneously both within and without the organizational structure and culture . . . we are educators and leaders and communicators within, and effective liaisons and open doors to those outside.”*

*Nuala O'Connor Kelly  
Speaking to the International Association of Privacy  
Professionals, October 30, 2003*

### **Education and Training**

One way to ensure that privacy is embedded into the culture of the Department of Homeland Security is through a vigorous education and training program. The Privacy Office recognizes the value and need for systematic privacy training at the Department and has spent the last fourteen months creating the framework for a comprehensive program.

Many of the agencies that merged with the Department had their own training initiatives and so the Privacy Office's work has included a survey of existing resources to ascertain how they might be leveraged for general Departmental use. In 2004, a Director of Privacy Compliance was hired to serve as the focal point of training and compliance initiatives.

The Privacy Office is now creating and implementing privacy awareness training for all DHS employees and new hires. The primary goal of privacy awareness training is to ensure that DHS employees are fully informed about how to handle personally-identifiable information in a responsible and appropriate manner. This program will not only be a requirement for all employees, but it will also set the baseline for subsequent awareness and communication campaigns by the Privacy Office. Subsequent training modules are planned that will be tailored to individual groups within DHS to ensure a broad agency understanding of how privacy integrates with specific DHS programs so that it is addressed appropriately.

### **DHS Privacy Advisory Committee**

As important as internal training initiatives are for DHS employees in order to foster an appreciation of privacy, equally important for the mission of DHS and for the Privacy Office is outreach, to bring in new ideas from outside the agency in order to provide for better informed decisions. One means of outreach that promises to be especially beneficial to the Privacy Office and to DHS is the Data Integrity, Privacy, and Interoperability Advisory Committee. The Committee will advise the Secretary and the Chief Privacy Officer on programmatic, policy, operations, administrative, and technological issues that affect individual privacy, as well as on data integrity and data interoperability and other privacy-related issues.

The Privacy Office solicited applications for the advisory committee in 2004. (See Appendix I) The Committee will be appointed by the Secretary and must be qualified to

serve by virtue of the education, training, or experience. The panel will include recognized experts in the fields of data protection, privacy, interoperability, and emerging technologies. Membership terms will be for a period of up to four years, with initial terms staggered to permit continuity and orderly turnover.

There is significant interest in this advisory committee; as of the date of this report, the Privacy Office received more than 125 applications for positions from a wide variety of qualified individuals. The Privacy Office intends to build a balanced but diverse advisory committee.

## **THE DEPARTMENTAL DISCLOSURE PROGRAM: IMPLEMENTING THE FREEDOM OF INFORMATION ACT**

*“Secretary Ridge has said that “fear of government abuse of information . . . is understandable, but we cannot let it stop us from doing what is right and responsible.” The antidote to fear, as he has said, “is an open, fair, and transparent process that guarantees the protection and the privacy of that data.” I commit to this Committee, to the American people whom we serve, and to our neighbors around the globe, that the Privacy Office is implementing this philosophy on a daily basis at the Department of Homeland Security.”*

*Nuala O’Connor Kelly  
Testimony before the House of Representatives  
Committee on the Judiciary, Subcommittee on  
Commercial and Administrative Law, February 10, 2004*

In the first year of the Department of Homeland Security’s inception, its Freedom of Information Act (FOIA) program has evolved to become an integral part of DHS operations.

Armed with interim FOIA rules a management directive outlining FOIA responsibilities for all DHS offices, and a statutory framework of broad agency disclosure mandated by FOIA itself, the Privacy Office provides overall policy guidance to more than 430 FOIA and Privacy Act personnel agency-wide. A Departmental Disclosure Officer, reporting directly to the Chief Privacy Officer manages this function.

The Departmental Disclosure Officer accepts all requests for records submitted pursuant either to the FOIA or the Privacy Act of 1974 for DHS Headquarters elements, consisting of the Offices of the Secretary and Deputy Secretary, Legislative Affairs, Public Affairs, Chief Financial and Information Officers, Private Sector, International Affairs, Counter Narcotics and State and Local Coordination, and the Management Directorate. Additionally, the Departmental Disclosure Officer serves as a conduit to DHS Directorates and component agencies, forwarding them FOIA and Privacy Act requests seeking records they maintain.

The DHS Directorates -- Science and Technology, Information Analysis and Infrastructure Protection, Border and Transportation Security, and Emergency Preparedness and Response – have their own separate FOIA personnel. Additionally, DHS components such as the United States Secret Service, the Coast Guard, U.S. Citizenship and Immigration Services, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement, employ FOIA officers and information specialists.

The DHS website, <http://www.dhs.gov>, contains information about the FOIA process to assist members of the public seeking to obtain records from DHS. The website includes instructions on where to send a FOIA request, the requirements for submitting a

FOIA request, and an estimate of how long it will take for DHS to respond to a FOIA request.

During fiscal year 2003, personnel working under the umbrella of DHS processed 160,902 FOIA requests (agencies that preexisted the creation of DHS merged on March 1, 2003). Seventy-two percent of these requests were answered with either a full release of records or a partial release, with the most common reasons for withholding information being privacy-related (Exemptions 6 and 7(C)) of the FOIA were used nearly 62,000 times). A more complete picture of FOIA operations at DHS is presented in the DHS Annual FOIA Report, which can be found on the Internet at: <http://www.dhs.gov/interweb/assetlibrary/FOIADHSFY2003AnnualReport.pdf>. (See Appendix J)

## IMPLEMENTING PRIVACY OVERSIGHT

Most of the agencies that merged with the Department of Homeland Security had personnel already in place to handle Privacy Act and FOIA matters, and these key staff have become part of a unified team of professionals dedicated to ensuring government transparency and privacy compliance. At the same time, the Privacy Office recognized that certain programs, because of their high visibility and impact, require the services of a designated Privacy Officer to ensure that personally-identifiable information, which is required for program operations, is collected and maintained in strict compliance with fair information principles.

Privacy Officers have been appointed for the US-VISIT Program, the Transportation Security Administration, which oversees a multitude of programs affecting the traveling public, and the National Cyber Security Division, which has programs that push the cutting edge of technology and thus have the potential significantly to affect privacy. These privacy officers report to the Chief Privacy Officer and to their organizations. They work closely with the DHS Privacy Office and their respective programs on a wide variety of privacy issues and initiatives, including development of PIAs, privacy policies, and privacy notices to inform the public about these DHS initiatives, to name a few. The impact of a dedicated Privacy Officer within these program and component areas is easily seen by reviewing their privacy accomplishments this past year.

### **The US-VISIT Program's Privacy Accomplishments**

The US-VISIT Program represents a major milestone in enhancing our nation's security and our efforts to reform our borders. It is a significant step towards bringing integrity back to our immigration and border management systems. It is also leading the way for incorporating biometrics into international travel security systems.

When fully implemented, US-VISIT will provide a dynamic, interoperable information system involving numerous stakeholders across the government. US-VISIT began implementing Increment 1, collecting and retaining covered foreign visitor's biographic, travel, and biometric information (inkless digital index finger scans and digital photographs), on January 5, 2004, at 115 air and 14 seaports.

The US-VISIT Privacy Officer, who can be reached at [usvisitprivacy@dhs.gov](mailto:usvisitprivacy@dhs.gov), is accountable for compliance with applicable privacy laws, regulations, and US-VISIT privacy requirements. Working with the DHS Privacy Office, the Privacy Officer is also responsible for creating and sustaining a culture within the US-VISIT program office, where privacy is paramount and fully integrated into the business and technology planning and development processes.

In close consultation and coordination with the Chief Privacy Officer, US-VISIT published a privacy policy on November 21, 2003, which can be found at <http://www.dhs.gov/interweb/assetlibrary/USVISITPrivacyPolicy.pdf>. The privacy policy explains the purpose of the program, who is affected, what information is collected, how

the information is used, who has access, how the information is protected, how long the information is retained, how to have inaccurate information corrected, and who to contact for more information. US-VISIT developed the privacy policy to help address critical privacy questions and concerns.

Although US-VISIT derives its capability from the integration and modification of existing systems of records, it nevertheless represents a new business process that involves new uses of existing data and the collection of new data items. As a result, and in an effort to make the program transparent as well as to address any privacy concerns that may arise as a result of the program, the Chief Privacy Officer worked with US-VISIT to perform a PIA in accordance with the guidance issued by OMB on September 26, 2003.

The US-VISIT PIA was published on January 4, 2004, and is available at [www.dhs.gov/us-visit](http://www.dhs.gov/us-visit). The PIA was hailed by many in the privacy community as an excellent model of transparency because it includes detailed information about the program, the technology and the privacy protections. (See Appendix F) The DHS Chief Privacy Officer and the US-VISIT Privacy Officer have met with numerous advocacy, privacy and immigration groups to solicit input and hear concerns. These concerns and recommendations have been taken into account in the development of the program and will be incorporated into future updates to the PIA as US-VISIT is further developed.

US-VISIT has established the basic organizational elements for its privacy program and now is in the process of defining roles and responsibilities and effective organizational interaction with key stakeholders. Going forward, US-VISIT intends to develop oversight and measurement capabilities, including a privacy compliance audit process to check progress towards meeting privacy goals.

In addition to the close working relationship maintained with the DHS Privacy Office, the US-VISIT Privacy Officer reports to the US-VISIT chief strategist in order to ensure that the privacy principles are applied to policies, standards, procedures, and guidelines. This is accomplished by developing and implementing requirements for privacy-compliant activities and operations including data usage agreements between US-VISIT and other agencies authorized to have access to US-VISIT data. Privacy principles are imbedded in the systems development and security architecture through administrative, procedural, physical, and electronic safeguards that control privacy risk. Awareness programs have also been instituted to make agencies, vendors, foreign visitors, and the public aware of the US-VISIT privacy principles and practices. Program monitoring and compliance auditing is being conducted to ensure adherence to the privacy principles, laws, regulations, and requirements.

US-VISIT has implemented a three-stage process for individuals to inquire about the data US-VISIT has collected in order to facilitate the amendment or correction of data that are not accurate, relevant, timely, or complete. The first stage in the process occurs at the primary inspection lane and provides on-the-spot data correction. A U.S. Customs and Border Protection Officer has the ability to manually correct the traveler's name, date of birth, flight information, and country-specific document number and document type errors. For data mismatches involving biometrics, the officer sends a data correction request to US-VISIT. The second stage allows for visitors processed through US-VISIT to have their records reviewed for accuracy, relevancy, timeliness, or completeness.

The US-VISIT Privacy Officer has set a goal of processing redress requests within 20 business days. Individuals who are not satisfied with the result can progress to the third stage by appealing to the DHS Chief Privacy Officer who will conduct an investigation and provide final adjudication. With nearly six million travelers processed through US-VISIT to date, only 31 individuals have inquired about their US-VISIT records. All of those inquires have been addressed and resolved by the US-VISIT Privacy Officer.

### **TSA's Privacy Accomplishments**

The TSA Privacy Officer, whose responsibilities consist of implementing the policies and directives of the DHS Chief Privacy Officer, began oversight activities of TSA programs in March 2004. Since that time, working in close coordination with the DHS Privacy Office, the TSA Privacy Officer has assumed an active -- and in fact, proactive -- role in ensuring that TSA programs are fully consonant with all privacy requirements.

For example, the TSA Privacy Officer has been closely involved in the planning and development of TSA programs that require the collection, use and disclosure of personal information, ensuring that the information collected is: (1) necessary; (2) properly stored; (3) securely transmitted; (4) disclosed only to those individuals with a "need to know;" and (5) that there are sufficient redress mechanisms in place for those individuals who are affected by the collection. Some of these programs include the Registered Traveler Pilot Program and the screening program for holders of licenses for transport of hazardous materials.

TSA has developed training materials for employees on various aspects of the Privacy Act as well as on TSA privacy policies that are applicable to every functional level of the agency. For example, in cooperation with the DHS Privacy Office, TSA developed training materials on the Privacy Act describing each employee's responsibilities with respect to the collection, use and disclosure of individuals' personally-identifiable information. This training, entitled "Respecting Privacy, Preserving Freedoms," is required for all TSA employees both at headquarters and in the field. Additional training is also being developed that will focus on DHS privacy policies and their applicability to the employee's job description.

TSA held a successful Privacy Week in spring 2004, at which all employees received mandatory privacy awareness training. Senior management from DHS and within TSA strongly supported the initiative.

The TSA Privacy Officer, working closely with the Chief Privacy Officer and Privacy Office staff, also has exercised strong leadership in ensuring the TSA programs complete and publish Privacy Impact Assessments related to various programs that are currently in prototype phase or have are being implemented. PIAs for the following programs have been completed:

- (a) Security Threat Assessments for Commercially Licensed Drivers with HAZMAT Endorsements (April 15, 2004; revised June 1, 2004)



- (b) Registered Traveler Prototype (June 24, 2004)
- (c) Airport Access Control Pilot Project (June 18, 2004)
- (d) Security Threat Assessment for SIDA and Sterile Area Workers (June 15, 2004)

The above-mentioned Privacy Impact Assessments have been published and can be found on the DHS Chief Privacy Officer's website ([www.dhs.gov/privacy](http://www.dhs.gov/privacy)). A number of other Privacy Impact Assessments are currently in progress and will be published by the end of the year.

The TSA Privacy Officer also is involved in other initiatives intended to ensure that privacy is at the core of TSA's mission. For example, TSA currently is reviewing data sharing with contractors, law enforcement, airlines and all other relevant parties inside and outside the agency in order to develop appropriate policies and employee guidance.

### **National Cyber Security Division – US-CERT Privacy Accomplishments**

The National Cyber Security Division (NCSO) has worked diligently during the last year, most notably through the leadership of its Privacy Officer, to help further the mission of the DHS Privacy Office in the context of the mission of the NCSO. The NCSO is tasked by the Secretary with the overarching responsibility to coordinate the implementation of the *National Strategy to Secure Cyberspace* and, consistent with the mandate of Homeland Security Presidential Directive 7, to serve as a focal point for the public and private sectors for cyber security. As detailed in the *Strategy*, our nation has become increasingly dependent on cyberspace for our national security, our economic well-being, and our law enforcement and public safety. With the increasing migration of personal information onto the interconnected network of information systems in the public and private sectors, it is more important than ever that we enhance the security of cyberspace to protect the privacy of all individuals.

NCSO is working to fully understand the privacy implications of its mandate and be cognizant of the possible impact on privacy of the implementation of its mission. In furtherance of its mandate, NCSO facilitates interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia, and international organizations. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems.

The NCSO operational arm is the U.S. Computer Emergency Readiness Team (US-CERT), a partnership between the NCSO and the private sector that was established to help protect and maintain the continuity of the Internet and our nation's cyber infrastructure. The overarching approach to this task is to facilitate and systemize global and domestic coordination of preparation for, defense against, response to, and recovery from, cyber incidents and attacks across the United States. To this end, while endeavoring to scrupulously respect privacy rights and obligations, US-CERT is building a robust cyber watch and warning capability, launching a public-private partnering effort to build

situational awareness and cooperation, and coordinating with Federal agencies, state and local governments, and the private sector. The overarching goal is to enhance America's ability to predict, prevent, respond to, and recover from cyber attacks and incidents, and the cyber consequences of physical attacks and incidents.

Operationally, NCSO-US-CERT has a privacy policy for the US-CERT website and is developing a privacy policy for the US-CERT HSIN Portal that is a secure collaboration vehicle in a pilot phase. NCSO also is working with the Privacy Office on privacy issues related to cyberspace situational awareness.

## **THE WAY FORWARD:**

### **A PERSONAL NOTE FROM THE CHIEF PRIVACY OFFICER**

America, it has been said, is a country of "rugged individualists." We asked in our Declaration of Independence that our government be a "new guard for future security," while at all times respecting the primacy of the individual's rights. Our Constitution, while not specifying a right to privacy, reflects the universal recognition that privacy is an important right, such that legal scholars recognize privacy as a "penumbral" Constitutional right. Our forefathers recognized that to have security, but not privacy, is insufficient. We share that recognition today.

Reflecting this philosophy, the Department of Homeland Security is not only a counterterrorism agency, but also, as Secretary Ridge has emphasized so often, a protective agency. The senior leaders of this Department, with whom I am proud to serve, are committed to safeguarding the people and places of our country, as well as our liberties and our way of life. A significant part of safeguarding those liberties is protecting the dignity and the uniqueness of the individual. And protecting the dignity and uniqueness of the individual requires -- indeed demands -- that we protect the privacy of that individual. It therefore has been my honor during the first year of the Department of Homeland Security's existence to help ensure that we protect the privacy of each individual, because I, like my colleagues in the Department of Homeland Security, recognize the absolute imperative to foster security while protecting individual privacy.

I close this report recognizing that we live in uncertain times. It causes me to consider a lesson from Thomas Jefferson, who noted, "It is part of the American character... to surmount every difficulty with resolution . . . ." With resolution and pragmatic optimism we will continue the crucial work of this Department and of the Privacy Office: to protect America and its many freedoms -- including individual privacy.

Thank you for the opportunity to serve and to report on privacy activities at the Department of Homeland Security.

Nuala O'Connor Kelly  
Chief Privacy Officer  
U.S. Department of Homeland Security  
Washington, District of Columbia  
July 2004

H. R. 5005

**One Hundred Seventh Congress**  
**of the**  
**United States of America**

AT THE SECOND SESSION

*Begun and held at the City of Washington on Wednesday,  
the twenty-third day of January, two thousand and two*

**An Act**

To establish the Department of Homeland Security, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

- (a) **SHORT TITLE.**—This Act may be cited as the “Homeland Security Act of 2002”.

(b) **TABLE OF CONTENTS.**—The table of contents for this Act is as follows:

**TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION**

**Subtitle C—Information Security**

**SEC. 222. PRIVACY OFFICER.**

The Secretary shall appoint a senior official in the Department to assume primary responsibility for privacy policy, including –

- (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
- (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- (3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
- (4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and
- (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.



## **U.S. Department of Homeland Security**

# **Privacy Office MISSION STATEMENT**

The mission of the DHS privacy office is to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while achieving the mission of the Department of Homeland Security.

The privacy office will achieve this mission through:

- Internal education and outreach efforts to imbue a culture of privacy and a respect for fair information principles across the department.
- Constant communication with individuals impacted by DHS programs to improve our understanding of DHS's impact, and, where necessary, modify DHS activities—through formal notice, constructive policy discussions, and complaint resolution mechanisms.
- Encouraging and demanding at all times an adherence to the letter and the spirit of laws promoting privacy, including the Privacy Act of 1974 and the E-Government Act of 2002,
- as well as widely accepted concepts of fair information principles and practices.



## Department of Homeland Security



### Nuala O'Connor Kelly Chief Privacy Officer

Nuala O'Connor Kelly was appointed Chief Privacy Officer of the Department of Homeland Security by Secretary Tom Ridge on April 16, 2003. In this capacity, O'Connor Kelly is responsible for privacy compliance across the Department. Her responsibilities encompass assuring that the technologies used by the Department to protect the United States sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal and Department information. The Privacy Office also has oversight of all privacy policy matters, including compliance with the Privacy Act of 1974, the Freedom of Information Act of 1966 (as amended), and the completion of Privacy Impact Assessments on all new programs, as required by the E-Government Act of 2002 and Section 222 of the Homeland Security Act. The Privacy Office also evaluates legislative and regulatory proposals involving collection, use, and disclosure of personal and Department information by the Federal Government.

Before joining the Department of Homeland Security, O'Connor Kelly served as Chief Privacy Officer for the U.S. Department of Commerce. While at Commerce, O'Connor Kelly also served as Chief Counsel for Technology, and as Deputy Director of the Office of Policy and Strategic Planning.

Prior to her beginning her government career, O'Connor Kelly served as Vice President-Data Protection and Chief Privacy Officer for Emerging Technologies for the online media services company, DoubleClick. O'Connor Kelly helped found the company's first data protection department and was responsible for the creation of privacy and data protection policies and procedures throughout the company and for the company's clients and partners. O'Connor Kelly also served as the company's first deputy general counsel for privacy.

O'Connor Kelly received her A.B. from Princeton University, a master's of education from Harvard University, and J.D. from the Georgetown University Law Center. She has practiced law with the firms of Sidley & Austin, Hudson Cook, and Venable, Baetjer, Howard & Civiletti in Washington, D.C. She is a member of the bar in Washington, D.C., and Maryland.



## Department of Homeland Security Privacy Office Leadership

### **Maureen Cooney** **Chief of Staff and** **Director, International Privacy Policy**



As the Chief of Staff for the Privacy Office, Ms. Cooney is responsible for assisting the Chief Privacy Officer in developing and representing the DHS Privacy Office policies, programs and goals. Ms. Cooney represents the Privacy Office both internally and externally, liaising with other federal agencies on privacy policy matters and federal implementation of privacy laws and regulations.

Ms. Cooney's responsibilities as the Director of International Privacy Policy include international policy development and counseling on international privacy law and policies. Cooney monitors DHS activities for international privacy impact and compliance with international arrangements, such as the U.S. – European Union Passenger Name Record Undertakings and Agreement. As part of her duties, Cooney represents the interests of the DHS at international meetings, including the International Conference of Privacy and Data Protection Commissioners and as a U.S. delegate to many multilateral organizations, as well as in bilateral dialogues with representatives of foreign governments and data protection commissions. Before joining DHS, Cooney worked on international privacy and security issues as the Legal Advisor for International Consumer Protection at the U.S. Federal Trade Commission. Ms. Cooney's government legal career has also included a litigation and counseling practice focused on financial services and enforcement issues, including extensive international work on anti-money laundering and foreign compliance issues, information sharing, and internal risk management, including privacy and security matters. Ms. Cooney received her A.B. degree in American Studies from Georgetown University and her J.D. from the Georgetown University Law Center.



**Elizabeth Withnell**  
**Chief Counsel to the Privacy Office**

As Chief Counsel, Withnell is responsible for providing legal advice on a wide range of information disclosure and privacy matters to the Chief Privacy Officer, the Privacy Office staff, and Departmental components. Withnell reviews all Privacy Office initiatives for legal sufficiency. She also represents the Department's privacy and disclosure interests at inter-agency meetings, assists with FOIA and Privacy Act litigation matters, and conducts reviews of DHS regulatory initiatives for compliance with privacy and disclosure mandates. In this regard, Withnell serves as the initial reviewing authority for DHS Privacy Impact Assessments which must be approved by the Chief Privacy Officer. Other previous experience includes more than a decade of FOIA administrative and litigation-related activities at the Department of Justice's Office of Information and Privacy, where she litigated FOIA cases in federal courts and provided FOIA training governmentwide. Withnell received her law degree with honors from Georgetown University Law Center. She is a member of the bar of the District of Columbia.



**Peter Sand**  
**Director, Privacy Technology**

As the Director of Privacy Technology, Sand coordinates the integration of privacy awareness and protections with the Department's development and use of information technologies. This is accomplished primarily through an ongoing dialogue with members of the Department's scientific and technology components. As technology-rich programs are developed within DHS, Sand ensures that privacy is one of the first and prominent issues considered. At the same time, Sand brings the details of the nature and use of technology back to the DHS Privacy Office to keep the policy and legal architecture of privacy grounded in the hard science of information technology. Before joining the DHS, Sand served as the Chief Privacy and Chief Information Officer for the Pennsylvania Office of the Attorney General. In the Office of Attorney General, Sand provided direct oversight of the specific technology used to support that office's law enforcement activities. In addition, Sand worked with senior law enforcement leadership in Pennsylvania as well that of other states and federal agencies to build an action-oriented strategy that integrated technology and policy. He has also practiced as an attorney and technology consultant to state and local government agencies and non-profit and educational organizations. Mr. Sand graduated from Villanova University and the Villanova University School of Law.



**Tony Kendrick****Director, Departmental Disclosure & FOIA**

As the Director of Departmental Disclosure and the FOIA Kendrick establishes FOIA and Privacy Act disclosure policy and regulations. He advises the Chief Privacy Officer on FOIA and privacy information release aspects of requests and systems planning. He also provides FOIA guidance to the more than 22 component offices and agencies of the Department and the more than 400 FOIA specialists processing more than 180,000 FOIA and Privacy Act requests each year. He ensures the development of public affairs guidance and training programs are consistent with Departmental policies and regulations and FOIA and Privacy Act training programs of the Privacy Office. His government career began in 1968 and included tours of duty with the military as an Army medic in Vietnam followed by an active duty and reserve military career as a Navy officer with public affairs and FOIA responsibilities. Concurrently with his reserve career he embarked on a government public affairs and FOIA career with the Departments of Defense, Agriculture, and Health and Human Services. Mr. Kendrick received a bachelor of arts degree in law enforcement and a masters degree in journalism (public relations) from the University of Maryland.

**Rebecca J. Richards****Director, Privacy Compliance**

As the Director of Privacy Compliance, Richards establishes and enforces privacy policy, including privacy impact assessment requirements, for the various electronic and records systems used by the Department. She accomplishes this by reviewing and identifying best practices across the various directorates' privacy education and training, policies, procedures, protocols, and protections that have been implemented as required by law and the Department and then implementing these best practices agency wide. In addition, her responsibilities include auditing programs to ensure they remain compliant with rules and regulations, and also international agreements, regarding the privacy of U.S. citizens as well as foreign visitors. Before joining the DHS, Richards was Director of Policy and Compliance at an independent non-profit privacy certification program for companies doing business on the web. She has also worked as an international trade specialist with the U.S. Department of Commerce and worked on the U.S.-European Union safe harbor accord. She received her B.A. from University of Massachusetts, Amherst, a Masters in international trade and investment policy, and an MBA from George Washington University.



## Department of Homeland Security Privacy Leadership



**Steven P. Yonkers**  
**US-VISIT Privacy Officer**  
**Border and Transportation Security**

Steven P. Yonkers has served since January 2004 as the Privacy Officer for the US-VISIT program of the Department of Homeland Security, within the Border and Transportation Security (BTS) Directorate. The BTS Directorate has the responsibility for securing the borders and transportation systems of the United States, enforcing the nation's immigration laws, and protecting government buildings and employees. As the US-VISIT Privacy Officer, Yonkers is responsible for ensuring that foreign visitor personal information collected, used, and maintained is safeguarded. Yonkers ensures that US-VISIT data is compliant with applicable privacy laws and regulations, as well as US-VISIT privacy requirements. He is also responsible for creating and sustaining a culture within the US-VISIT program office where privacy is paramount and fully integrated into the business and technology planning and development processes. Before joining US-VISIT, he served with the U.S. Immigration and Naturalization Service and the U.S. Department of Justice, and worked in the private sector. Mr. Yonkers received his A.B. in Sociology from Ohio University and a master's of science from American University in Criminal Justice Administration.



**Lisa S. Dean**  
**Privacy Officer, Transportation Security Administration**  
**Border and Transportation Security**

Lisa S. Dean serves as the Privacy Officer for the Transportation Security Administration (TSA), within the Border and Transportation Security (BTS) Directorate. The BTS Directorate has the responsibility for securing the borders and transportation systems of the United States, enforcing the nation's immigration laws, and protecting government buildings and employees. Vital to the BTS mission is protecting the nation's transportation systems and infrastructure and the people who operate them and passengers who use them, this goal is carried out by the TSA. As the TSA Privacy Officer, Dean oversees TSA compliance with federal privacy laws and DHS agency-wide privacy policies with regard to the collection, use, and dissemination of personally identifiable information and establishing complementary privacy policies for TSA. Ms. Dean joined the federal government following employment in the private sector where she gained experience in privacy protection and access issues, and she organized a coalition to advocate for stronger federal and state privacy protections for personal information.



**D. Andy Purdy**  
**Privacy Officer and**  
**Deputy Director, National Cyber Security Division**  
**Information Analysis and Infrastructure Protection**

Donald Andy Purdy is the Deputy Director of the National Cyber Security Division (NCSA) for the Department of Homeland Security, within the Information Analysis and Infrastructure Protection (IAIP) Directorate. The IAIP Directorate identifies and assesses a broad range of intelligence information concerning threats to the people and communities of the United States and protects critical infrastructure systems vital to our national security, governance, public health and safety, economy, and national morale. As the Deputy Director for NCSA, Purdy helps to further the NCSA mission to coordinate the implementation of the *National Strategy to Secure Cyberspace*, a strategy he helped develop while assigned to the White House staff, and serves as a focal point for the public and private sectors for cyber security issues. Before joining the Department, Purdy worked in the areas of cyber crime, privacy protection, government procurement and maintenance of more secure products and systems, security of the financial sector's information systems, and in promoting information sharing in the industry sectors such as health care and finance. Mr. Purdy graduated from the College of William and Mary and the University of Virginia Law School.



**“A Safe and Open Society”**

Keynote Address

of

**NUALA O’CONNOR KELLY**

**CHIEF PRIVACY OFFICER**

**U.S. DEPARTMENT OF HOMELAND SECURITY**

Before the

**25<sup>th</sup> International Conference of**

**Data Protection and Privacy Commissioners**

Sydney, Australia

September 11, 2003

Good morning. It is a great honor to be with all of you at this gathering of distinguished colleagues and leaders in the international privacy community. First let me thank Commissioner Malcolm Crompton, our host at this gathering, who kindly extended the invitation for me to address this group. I would also like to recognize Monsieur Michel Gentot of the Commission Nationale de l’Informatique et des Libertés, our guide for this session.

It is my great pleasure to also recognize my many distinguished friends and colleagues from the United States of America, from both the public and private sector, who have traveled to be part of the important dialogues taking place at this conference. In particular, I would like to recognize Commissioners Orson Swindle and Mozelle Thompson of our Federal Trade Commission, who have been leaders in the United States’ participation in the international data protection dialogue. I’d also like to take a moment to recognize the professional staff of the Federal Trade Commission, so many of whom have become my colleagues and friends in my time in Washington—some of whom are here today, like Maureen Cooney, and others who are back home working while we are all here enjoying the glory of this beautiful country. And of course our many private-sector colleagues, like Marty Abrams of the Center for Information Policy Leadership, who constantly challenge all of us in the privacy community in the United States to do better.

*September 11: Remembering Our Fallen Patriots*

And it is impossible to speak on this date, without recognizing the tragic events of just two years ago, and honoring the memories of the more than 3,000 people who lost their lives on this day. As many of you know, while I am a native of Belfast, Northern Ireland, I have spent most of my life in and around New York City, and I will probably forever, no matter where I live, consider myself a New Yorker. My family was personally affected by these events, and I also had many friends in and around the World Trade Center.

Citizens of more than eighty countries died on September 11, 2001 in New York, Washington, and Pennsylvania.<sup>1</sup> To put that number in context, almost every country represented in this room, plus an additional 58 countries, lost a citizen on September 11.

For the victims of these attacks, and for the victims of the more recent attacks in Bali and Jakarta, and for the victims of terrorism around the world, I ask you to join me in a brief moment of silence.

The 17<sup>th</sup> century English poet, John Donne, wrote that: "Any man's death diminishes me, because I am involved in mankind." The deaths that occurred on September 11, 2001 diminish all of us because their killers sought to end not only their lives, but to quash the very safe and open society that is the title of our discussion today. This, the largest single terrorist act in modern history, requires us to face those who would seek to diminish a free and welcoming society—one where, on a given day in September, the name of those buildings—the World Trade Center—had real meaning. We—as individuals, as people—must face those who would end freedom of speech, freedom of association, freedom of religion, freedom of commerce, and we must stand for this free and complex society in which we believe.

I know and have heard that many of you are concerned that the United States' reaction to these events has put privacy and civil liberties to the test in our country. But you must know as well that the foundations of privacy and the love of civil liberties run far and deep into the bedrock of our country. I'd like to share with you today both a historical perspective on the underpinnings of our free and open society, and to also tell you about our more modern approaches to government respect for individual privacy.

---

<sup>1</sup> Antigua & Barbuda, Argentina, Australia, Austria, the Bahamas, Bangladesh, Barbados, Belgium, Belarus, Belize, Bolivia, Brazil, Cambodia, Canada, Chile, China, Colombia, Costa Rica, Czech Republic, Dominica, the Dominican Republic, Ecuador, Egypt, El Salvador, France, Germany, Ghana, Greece, Guatemala, Guyana, Haiti, Honduras, Hong Kong, India, Indonesia, Iran, Ireland, Israel, Italy, Jamaica, Japan, Jordan, Kenya, Lebanon, Luxembourg, Malaysia, Mexico, Morocco, the Netherlands, New Zealand, Nicaragua, Norway, Pakistan, Panama, Paraguay, Peru, the Philippines, Poland, Portugal, Romania, Russia, Slovakia, South Africa, South Korea, Spain, Sri Lanka, St. Kitts & Nevis, St. Lucia, Sweden, Switzerland, Taiwan, Thailand, Trinidad & Tobago, Turkey, the Ukraine, the United Kingdom, the United States of America, Uruguay, Uzbekistan, Venezuela, Yemen, and Zimbabwe.

#### Foundations of American Freedom: The Primacy of the Individual over the State

From our very Declaration of Independence in 1776, the American psyche has been one which values the rights of the individual over government control. This country has been described as one of "rugged individualists," and our Declaration complained of, and sought emancipation from, "a long train of abuses and usurpations" by the government. This seminal document states of the individual that it is "their right, it is their duty, to throw off such Government, and to provide new Guards for their future security." Interestingly, while most Americans speak of "life, liberty, and the pursuit of happiness" as their individual rights under the Declaration, it is as a "new guard for their future security"—in the so many senses of that word—that is the anticipated, and limited role of a free and just government described by the Declaration. That in this limited role, government is not above laws and man, but rather a creation of law and man, and thus subject to them, is a fundamental underpinning of this document. The first of the litany of offenses against the King in the Declaration were that "He has refused his Assent to Laws, the most wholesome and necessary for the public good." It is not required then, by our Declaration, that government be ineffective, but rather, that it promotes a greater good, and that it be a "new guard for [our] future security," while at all times realizing and respecting the primacy of the individual's rights.

Some thirteen years later, the United States Constitution and the amendments thereto formalized the structure for what the federal government would become. And for those of us working in the government, it is a healthy thing to refer back frequently to the document that created these structures. On a more personal note, I keep, as has been now reported in the US press, a copy of the section of the Homeland Security Act that created the Privacy Office taped to the wall in my office so I can refer to it constantly. It's a good reminder of what the Congress intended for my job and my office to be about. But I digress.

In the preamble to the Constitution, the purpose for this document is articulated: "We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America." It is a fascinating thing, at a time when our friends in the European Union are in the process of drafting a Constitution themselves, to reflect upon the values that are the foundation of this document. The Bill of Rights, contained in the Amendments to the Constitution, further articulates the rights of the people to freely exercise their religion, to

freedom of speech, to freedom of the press; to peaceably assemble, to petition the government for a redress of grievances. to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." However, the Ninth Amendment also states that "the enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people."

There is no stated right to privacy in the United States Constitution. But it is an underpinning, a theme, a universal recognition, that has led scholars to describe privacy as a "penumbral" right within the constitution.

#### American Jurisprudence on Privacy

There is a long, rich, and complex history of judicial pronouncements on privacy in the United States. Author Sheldon Richman wrote in 1993 that "no question in jurisprudence is as muddled as that of privacy." Richman argues for privacy as a property right, a popular viewpoint-or at least a popular analogy-in the United States. However, an even more prevalent viewpoint than the proletarian one in American jurisprudence, and one that continues to be expounded on by our own Supreme Court, is privacy as "the right to be left alone," a standard first articulated in 1890 in an article in the Harvard Law Review written by esteemed jurists Louis Brandeis and Samuel D. Warren. In that article, Justices Brandeis and Warren argue not for "the principle of private property, but that of an inviolate personality."

To have an inviolate personality, or rather, the ability to create a personality or persona for the outside world, is again, I believe, a part of a uniquely American psyche. The power to invent and reinvent one's self can be seen in our cultural icons from F. Scott Fitzgerald's *The Great Gatsby* to present-day pop icons like Madonna. One's choice to reveal or not reveal, and the power to control not only one's personal life and public career, but also to control the information that surrounds one's life, perhaps is not so uniquely American, but rather, is universal. But the power to be unmoored and unshackled from one's social, cultural, economic, or class stratification, and to create an entirely new and different persona, however, does seem to me, at least, a fairly American phenomena-certainly one that is caught up in the American fascination with all things new, with our power to invent, and our power to control our own destiny. And to do that, to create a persona without regard to traditional signposts of family or background or history, rests definitively on a certain measure of personal control over one's defining information and choices. Justice Brandeis later wrote, in 1928, in *Olmstead v. United States*, that the Constitution "conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men."

Much later in this century, a string of Supreme Court cases on privacy again tested our concept of the right to be let alone. Beginning in the 1960s, the Supreme Court considered a number of cases and alternately struck down and upheld various personal choices having to do with that most private act--of sexual intercourse. In 1965, the U.S. Supreme Court struck down a law from the State of Connecticut which prohibited the use of contraceptives by married couples. The Court cited the "preeminence" of the home as the "seat of family life" as entitling a "zone of privacy," as its rationale for permitting the use of contraception. Following that decision, in 1973, in one of perhaps the Supreme Court's most well-known privacy cases, *Roe v. Wade*, the Court recognized a limited right to abortion. And in two recent cases, the court first upheld, and then struck down, state laws prohibiting sodomy, first in *Bowers v. Hardwick* (1986) and then *Lawrence v. Texas* (2003), redefining, most recently, a right of privacy in one's romantic, sexual, and familial matters, regardless of sexual orientation.

It was in the *Griswold* case, I believe, that the concept of a penumbral right of privacy-one that surrounds and is created at the intersection of various articulated rights-was created or articulated. In this articulation, privacy, though not expressly addressed in the Constitution or Bill of Rights, is an essential element necessary to achieving the rights articulated in our constitution. It is almost as if the framers thought it was so obvious that it didn't need to be written down.

#### Legislative Thought on Privacy

At around the same time *Roe v. Wade* was being decided by the United States Supreme Court, concepts of fair information principles were being explored in Europe and throughout the world. Just a year after this landmark court case, the United States' federal Privacy Act of 1974 was passed. Growing out of universal concerns about the growing aggregation of personal information--partly due to new technologies like mainframe computers--and perhaps also out of the Watergate scandal and other governmental issues of the day--this law provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, through detailed "system of records" notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one's own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records.

Under the Freedom of Information Act, the principle that persons have a profound and fundamental

right to know what their government is doing is upheld--almost in the extreme. Any person at any time has the right to query a federal agency about documents and records. A modest fee may be assessed for the time and effort in compiling those records, and in some instances, that fee is waived. While this right is quite frequently exercised by non-U.S. persons, or citizens of other countries, it is most frequently exercised by members of the press. The U.S. federal government will spend tens of millions of dollars processing and responding to FOIA requests next year, and thousands of federal workers will spend all or part of their day compiling responses to those requests.

A third pillar of the privacy framework at the federal level reflects, once again, a growing reliance on technology to move data--both in government spaces and on the Internet. The E-Government Act of 2002 contained a landmark requirement for privacy impact assessments by federal government agencies.

The provisions of the E-government act set forth a comprehensive framework for considering privacy in the ordinary course of business of government--serving our citizens. The Act and underlying guidance synthesize a myriad of prior guidance on privacy practices and notices, and will assist privacy practitioners in prioritizing their efforts. In particular, the guidance provides helpful information on the content of privacy notices and topics for required disclosure.

Further, the act requires the parameters for privacy impact assessments. Although in use by some agencies already, generally privacy impact assessments are a new and important tool in the tool belt of privacy practitioners across the federal government. These new requirements formalize an important principle: that data collection by the government should be scrutinized for its impact on the individual and that individual's data...and ideally before that data collection is ever implemented. The process, the very exercise of such scrutiny, is a crucial step towards narrowly tailoring and focusing data collection towards the core missions of government. This practice should provide even greater awareness, both by those seeking to collect the data and those whose data is collected, of the impact on the individual and the purpose of the collection.

I am pleased to have been a small part of the discussions towards the development of guidance on privacy impact assessments. These new requirements set the bar high for privacy practitioners. These requirements also reflect, I believe, a growing sensitivity and awareness on the part of our citizens regarding personal data flows in the public and private sectors. I believe that this guidance will allow federal agencies to respond to citizens' concerns about these activities and also to be current with, or perhaps even

slightly ahead of, the evolution of privacy practices in the private sector.

Under the Privacy Act, in concert with the Freedom of Information Act and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them.

#### Administrative/Enforcement Efforts on Privacy

The United States has, I am told, been criticized for a lack of an omnibus privacy statute. But in the federal government space, at least, one certainly exists, and that is the Privacy Act of 1974. In the private sector, privacy principles are slightly harder to explain, in that there is not one single piece of legislation. However, I would joyfully and passionately pronounce that while the legislative framework is complex, the enforcement--from a multitude of sources--is tremendous and zealous. In fact, it is this multiplicity of sources--legislative, judicial, federal, state, and local, and not to mention the ever-present press--that makes me so proud of our commitment to privacy and fair information principles, both in the government and the private sectors.

At the federal level, as you already know, a strong commitment has been made by those who regulate the private sector, such as our friends at the Federal Trade Commission, the federal banking agencies, and the Commerce Department.

The United States' approach, as many of you have heard, is a sectoral one. As the string of judicial pronouncements have focused on sensitive sexual behavior and information, the legislative framework has focused on sensitive information used by regulated industries, particularly financial services and the healthcare industry.

In the banking sector, the one with which I am most familiar since I began my career as a banking lawyer, we have federal and state bank and insurance regulatory agencies which oversee and enforce a multitude of statutes affecting how financial institutions behave. The Fair Credit Reporting Act and the Gramm Leach Bliley Act each function at the federal level to limit the collection and use of sensitive personal financial information by private actors in the lending space. In addition to GLBA and FCRA, however, there are other federal consumer protection laws in the banking arena that safeguard sensitive information and empower consumers. The Equal Credit Opportunity Act, the Truth in Lending Act, the Electronic Fund Transfer Act, and the Fair Debt Collection Practices Act, and the multitude of regulations under these statutes, each in some way reinforces the importance of disclosing to consumers how their information will be used or affords consumers clear means for checking and correcting information that may cause financial harm.

State consumer protection laws as well as banking and insurance laws, and the respective commissions that enforce these laws, also play a role in enforcing fair dealings with the consumer, including the use of the consumer's information. This is far more than a system of best practices and principles. This is a system of regular, on-site compliance examinations by regulators, a system which can impose fines of up to \$1 million a day for the most egregious of infractions. This is a system that has bite.

The system of access and redress that has been created under the Fair Credit Reporting Act allows individuals to ensure the accuracy of their data while also providing accurate, equal, and secure information to banks and lenders who seek to make everything from credit cards to home mortgages more readily available. This system is one of the most robust access mechanisms to personal data, and has provided confidence in the U.S. consumer credit system that has made it one of the most vibrant in the world. The Fair Credit Reporting Act and the Equal Credit Opportunity Act have ensured that we as a country have provided equality of opportunity regardless of race, gender, ethnicity, or national origin to what we consider one of the most fundamental elements of the "American Dream," the ability to own one's home. We as a country, at least those of us who have only been in the credit marketplace since the Act first passed in the early 1970s, take for granted that ours is a safe, secure, and equitable system that is a platform for opportunity and advancement while also protecting the privacy and the sanctity of some of the most sensitive of our personal data. The Bush Administration, as many of you may know, is seeking to ensure that the uniform national standards in the FCRA are not only maintained, but are enhanced by affording consumers some significant new tools targeted at preventing, detecting, and recovering from the crime of identity theft, the fastest growing financial crime facing American consumers today.

The Health Insurance Portability and Accountability Act of 1996--and its thousands of pages of privacy regulations--provide greater protections for citizens than ever before in the use of their sensitive health records. President Bush's decision to move forward with this health privacy rule marked one of the first privacy-enhancing decisions of his Administration. HIPAA's Privacy Rule--still a relatively new set of regulations in its active enforcement--requires that health care providers give individuals greater insight about the use and disclosure of their medical records, greater access to those records, and enhances the individual's ability to control the use and dissemination of those records. The new rules also provide for federal oversight where an individual believes her health privacy rights under the new rules have been violated.

The Children's Online Privacy Protection Act and a host of other related laws protect the privacy and security of our children online. The Department of Commerce's Technology Administration--where I served as chief counsel before joining the Department of Homeland Security--and the National Telecommunications and Information Administration--have worked towards enforcing these principles online both through legislation and also through encouraging self-regulatory frameworks. The Commerce Department has recently been involved in creating a "safe space" for children online through a "dot-kids" domain. And of course my good friends at the International Trade Administration continue to work closely with many of you here today on international commercial data protection frameworks.

The Commerce Department, and even more importantly, privacy professionals from the private sector, have worked closely with groups like TRUSTe and BBB Online to promote best practices and principles. The private sector is particularly to be commended for advancing the dialogue on privacy in the United States, both by appointing senior-level officials whose primary role is to advocate privacy-enhancing decisions for their corporations, and for adopting a self-regulatory approach, through formal seal programs and smaller industry-sector working groups. This approach may be harder to explain, but the marketplace, as both an instrument of sanction for privacy offenders and would-be offenders, and as a forum for innovation, in both technology and policy, to meet privacy needs, has proven one of the greatest forces for privacy advancement.

And we cannot forget our friends at the Federal Trade Commission and their important work. The Federal Trade Commission is the only Federal agency with jurisdiction to enhance consumer welfare and protect competition in broad sectors of the economy. It enforces the laws that prohibit business practices that are anticompetitive, deceptive, or unfair to consumers, and seeks to do so without impeding legitimate business activity. The FTC also promotes informed consumer choice and public understanding of the competitive process. The agency's work is critical in protecting and strengthening free and open markets in the United States, and, increasingly, internationally.

And who among us--certainly not I, who has sat across the table as the representative of a company that was on the receiving end of an FTC investigation--could overlook their enforcement of Section 5 of the Federal Trade Commission Act. Thanks to the championing of Commissioners Swindle and Thompson and others, under the leadership of Chairman Timothy Muris, the Federal Trade Commission has continued, and in fact, drastically increased, the number of staff devoted to enforcement of unfair and deceptive trade practices in



the privacy area. Chairman Muris, as he recently explained in his remarks at the Progress and Freedom Foundation meeting in Aspen, Colorado, seeks to focus on harms, such as identity theft, nuisance, and fraud that arise from violations of privacy and the misuse of personal information in the commercial space.

And this is just at the federal administrative level. A host of state attorneys generals have sought to enforce state unfair and deceptive trade practices acts in the privacy arena. A number of states have constitutional privacy protections. And a host of litigators and class action lawyers have pursued privacy violations, both real and imagined, against corporations on behalf of individuals and groups. This multiplicity of federal, state, local, judicial, legislative, administrative, and regulatory enforcement mechanisms is no doubt complicated. But it also leaves individuals with a multitude of avenues to pursue and redress wrongs.

#### Privacy and the Homeland Security Department

And so, we have evolved from the right to be let alone, to personal privacy in the bedroom, to freedom of choice in the doctor's office, to online privacy, to now, in the days after September 11, a growing concern about the intrusion of our federal government in the name of Homeland Security.

It is surely one of the greatest honors that I will experience in my career--to have been chosen to serve as our country's first statutorily mandated Privacy Officer. And it is certainly no accident that the first privacy position created by Congress has been placed at the Department of Homeland Security. This new Department, formed largely in response to the events of September 11, 2001, encompasses the work of 22 former federal agencies and 182,000 federal employees. There is no question that the use of personal information about citizens and visitors to our country is fundamental to the department's mission.

This new Homeland Security Department includes the Coast Guard, the Secret Service, the border and customs agencies, a science and technology research unit, an information analysis section, an infrastructure protection division--focused on improving and hardening arteries--both old, like our power and utilities grids, and new, like the Internet. The Homeland Security Department includes the Emergency Preparedness and Response directorate--including an organization known as the Federal Emergency Management Agency, or FEMA, whose sole mission is to assist Americans in being prepared for, and being able to respond to, disasters of any variety, including terrorist attacks.

This department employs tens of thousands of federal workers whose primary job is to prevent the entry of transmission of dangerous goods or persons to our country. These are the men and women who have

been described as "standing on walls." They are those who are vigilant, at the borders, in our waters, at our points of entry. They protect us, they educate us, and they assist us when disaster strikes. It is my office's job to ensure that such activities are performed, at all times, with the greatest respect for the individual--regardless of citizenship, age, race, gender, national origin, or ethnicity. But the very performance of these jobs shows respect for the dignity of the individual--the dignity of that person's right to live safely and move about freely--free not only from unwanted or inappropriate government intrusion, but free also from the physical threats of those who would do them harm simply because they are in America or because they are Americans.

Homeland Security truly means what it is named. Though created out of the ashes of September 11, it is not solely a counter-terrorism agency. Though focused on the tangible assets of our country, such as borders and transportation systems, it is about more than just things--the mission of this department is to protect and defend the homeland in all its facets--both tangible and intangible. As Secretary Tom Ridge has said, this Department is not just about protecting America's assets. It's about protecting America.

Many people thought, when I took this job, that I had a hard job, maybe even an impossible job. But after meeting Secretary Ridge, I knew that while the issues and decisions were going to be hard, it was by no means going to be an impossible job, because, as I like to say, Secretary Ridge "gets it." Secretary Ridge understands what it means to be an American, to have freedom of choices and determine one's destiny. He understands, as does, I believe, the entire senior leadership at the department, the importance of not losing the intangible qualities that make America great, while we strengthen our physical defenses against those who would quash freedoms.

It is clear to me from my work side-by-side with the senior leadership of this department that we are all equally committed to creating a safe society, and each of us has a role in that mission. While safeguarding the people and the places of our country, we must also maintain the liberties and the way of life that have made this country a symbol of freedom and opportunity for people around the world. Part of maintaining those liberties is safeguarding the dignity and the uniqueness of the individual--and protecting the privacy of that individual.

In a speech, just a few days before I joined the department, Secretary Ridge articulated his vision for how the Department of Homeland Security would work with my office: that the privacy office "will be involved from the very beginning with every policy initiative and every program initiative that we consider," to ensure that our strategy and our actions are consistent with not

only the federal privacy safeguards already on the books, but also "with the individual rights and civil liberties protected by our laws and our Constitution."

I am very much in agreement with the statutory definition of my office's position as being both "within" and "without" the Department of Homeland Security. As part of the department, we are able to serve as educators, as leaders, and as full participants in the policy direction of important programs. And as outsiders, we are able to turn a critical eye on the most controversial and the most mundane aspects of the Department's operations. But I do not position my office as the enemy of the mission of this department. Rather, I see it as crucial, fundamental. The protection of privacy is neither an adjunct nor an antithesis to the mission of the Department of Homeland Security. Privacy protection is at the core of that mission.

And the Secretary has thought about, as I obviously do every day, what it means to use personal information in the federal government space-as custodian of the public's security, information, and trust. Secretary Ridge, in a speech to the Association of American Universities, said that "Fear of government abuse of information...is understandable, but we cannot let it stop us from doing what is right and responsible." The antidote to fear, he suggests "is an open, fair, and transparent process that guarantees the protection and the privacy of that data." He is in complete agreement with the advocacy community, with which I work so closely, to bridge the gap between those on the inside and the outside. A dear friend and colleague from one of our leading advocacy groups formulated his thinking this way to me recently: "We recognize that there will be elements of the Department's work that must, by definition, not be part of the public realm. But to compensate for those highly sensitive activities, the process towards creating those policies or programs must be that much more transparent, and the protocols for oversight must be that much more stringent, to make up for the lack of public scrutiny, of government in the sunshine, that we all hold so dear."

Secretary Ridge has pledged, and I will agree that "we will work together to ensure that our new programs appropriately use information, that we protect it from misuse, and that we discard it when of no further use."

Most importantly, our entire leadership pledge that in the course of protecting our homeland "we will not, as Benjamin Franklin once wrote, trade our essential liberties to purchase temporary safety. We must and we will be careful to respect people's privacy and civil liberties."

I am truly honored to be a part of the team of dedicated and passionate professionals at the Department of Homeland Security, and to be a part of the important mission of protecting this country. I can think of few more important missions for a federal

government than to keep our country and our citizens safe. And few more important tasks within that mission, than protecting the quality of what it means to live free in America, truly one of the most open societies that history has witnessed.

#### Role of the Privacy Officer

The Department of Homeland Security privacy officer is the first Congressionally created, statutorily defined privacy office the federal government. The statutory description of the job encompasses not only Privacy Act compliance efforts, but also the evaluation of emerging technologies for privacy impact, as well as the evaluation of legislative and regulatory proposals on privacy. Importantly, the Homeland Security Act, in which my office was created, specifies the completion of privacy impact assessments of proposed rules of the Department as part of the duties of the privacy officer. The Act also articulates the need to review legislative and regulatory proposals across the Federal government, also, importantly and uniquely, provides for a direct reporting relationship between my office and the United States Congress.

Even more than statutorily defined and required roles, however, a privacy officer is an agent for communication and education across the organization. I am creating a team that embeds privacy awareness into the structure and the culture of the organization. That will be accomplished not by one person alone, but rather by working side-by-side, as I've already begun to do, with the policy, legal, systems, and other professionals across the organization to embed an awareness that exceeds the confines of a privacy office. It is a new and different framework, I understand, to have a privacy office within a Department, or as other countries would describe, a ministry. But this is no usual ministry. Encompassing 22 former agencies, the Department of Homeland Security seeks to meld historic agencies--like the Customs Department, which, any employee will tell you, is mentioned in the Constitution and dates back to 1789--with new agencies, like the Transportation Security Administration, created in 2001. How to fit these units together so that their missions, their cultures, their operations are both streamlined and made more effective is an historic challenge and a historic opportunity. Not since World War II has the federal government in the United States sought to reorganize, become more effective, and rededicate itself to a new mission.

How wonderful an opportunity to have joined the department just six weeks after it opened its doors. What a daunting task to embed a culture of privacy into an organization which is currently redefining its culture. But what better time than now? What better way than to be part of the leadership team--to inform decisions, to advise and counsel, to debate and argue when necessary,

but to be perceived as an ally, an element, not only as an outsider, or a watchdog (which is also partially what I am, and certainly how I've been described).

The role of the Privacy Officer is to be both within and without. To sit on that wall, to look over and see and hear and ingest the complaints, the concerns, the demands of those outside-citizen and non-citizen alike, and to bring those concerns back inside-and operationalize them, make them real, inform the decision making process in a positive and proactive way. And conversely, to be the vehicle for transparency, accountability, and fairness, through Privacy Act notices that really describe new technologies in plain language that people, even those who didn't go to law school, can understand.

#### Internal Resources

It is a wonderful role. It is a joyous thing that the members of Congress created this role, and that, even more, the leadership of this Administration and this Department have embraced it. And it is not just an effort of one person. On my team, in the coming months, our headquarters staff will include not only lawyers, but technologists and policy makers who speak with both domestic and international expertise on data protection and privacy. In addition to our headquarters staff, throughout the component parts that now make up the Department of Homeland Security, we already have over 300 employees working full-time on Privacy Act and FOIA compliance work. The total budget allocated towards fulfilling the department's statutory mission on Privacy, including Privacy Act and FOIA compliance will exceed \$10 million dollars in 2004. And these numbers do not even consider the hundreds of dedicated civil servants in the legal department, on the chief information officer's team, in the management directorate, or throughout the policy shops and program development and technical development offices throughout the department, whose critical work assists my team in creating privacy impact assessments and Privacy Act statements. I am counting on each of these, and many others, to help us educate all of the employees of this vast new organization that their jobs can be performed effectively, zealously, and fully, while at all times respecting the dignity and the sanctity of the individual. I know it can be done.

#### External Dialogue

And just as we are fully engaged internally, the privacy office must also be part of the external dialogue, and that is why I am with you here today. It is certainly an important challenge, to achieve the security that we need to grow and flourish as a country, as an economy, as a community, while also protecting the rights and the privacy of the individual.

Just as the defense of our homeland is a responsibility that we all must embrace, so, too, is engaging in the debate over how to achieve security

while protecting privacy. In fact, our ability to have a free and open debate is a direct result of the freedoms that are at the bedrock of our society. And our willingness to engage in this conversation is, again, a sign of support and respect for our colleagues, our citizens, and our country.

We will achieve a free and open and transparent dialogue and information sharing about federal government through a variety of channels. In the most formal way, agencies are required to publish Privacy Act notices and Privacy Impact Assessments on new uses of technology and new collections of personal information. As you have already begun to see in notices about programs like the Computer Assisted Passenger Prescreening System or CAPPs II, we have endeavored to make these notices meaningful, robust, educational, and to provide true transparency as to intent. We have provided in these and other notices a fulsome view of the types of data intended to be collected, the purposes for which the data is collected, the data retention mechanisms in place, and the access and redress mechanisms. We have attempted to clearly define the purpose limitations for these systems, and have looked to Congressional language and intent for narrowly drawing these frameworks. Importantly, we have pledged that to the greatest extent possible, these access mechanisms will be equal for all persons, regardless of citizenship.

We have provided, through these notices, a lengthy comment and dialogue period--more than is required by law. We have opened and engaged in the debate formally. We have also provided not only the usual fax and postal mechanisms for commentary, but we have even provided an email address. One day last week, my office--and that includes the personal computer on my own desk--received 7,000 comments on one of our notices. That's more than 100 times the usual number of comments received to these types of notices during an entire comment period--and that was just one day during the 60-day period.

I have endeavored at all times to have an open door--and not just to those in Washington, and not just those in the data protection community. We must hear from ordinary citizens what their concerns are--and directly, not just through groups that seek to represent their interests.

I have encouraged all parties--citizens of the United States and other countries, members of Congress and members of Parliaments, data protection authorities from around the world--to engage with us, in a positive, productive, and also civil way. I believe that we can move forward together to achieve our mission of protecting and defending our lives and our way of life, preserving the liberties and freedoms--including that right to be left alone--that we all hold so dear. I encourage you, my colleagues in the data protection

community, to place yourselves at the center of your internal debates on governmental use of information, whether in the security, law enforcement or counter-terrorism arenas. It is frankly, a harder, but more important place to be, than remaining on the sidelines and pointing fingers.

I am honored and pleased to find myself once again at the center of this debate over the privacy, the sanctity of the individual in our increasingly complex information society. It is a great debate, a great challenge, and a great opportunity to serve the people of our countries.

It is often questioned, as we've said, whether we can achieve both security and privacy. To this, I of course, answer a resounding YES. The framers of our Constitution clearly thought so: their enumerated list of purposes for government included: establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, AND secure the Blessings of Liberty to ourselves and our Posterity. It is my great hope, and my great belief, and my job, to ensure both domestic tranquility and to secure the blessings of liberty to ourselves and our posterity. Anything less is a failure of our social contract, a failure of our mission, and a failure to advance a safe and open society. And I can assure you, in this, too, we will not fail.



WRITTEN TESTIMONY  
of  
**NUALA O'CONNOR KELLY**  
**CHIEF PRIVACY OFFICER**  
**U.S. DEPARTMENT OF HOMELAND SECURITY**

Before the  
**COMMITTEE ON THE JUDICIARY**  
**SUBCOMMITTEE ON COMMERCIAL AND ADMINISTRATIVE LAW**

UNITED STATES HOUSE OF REPRESENTATIVES

February 10, 2004

Chairman Cannon, Ranking Member Watt, Members of the subcommittee, and distinguished colleagues on this panel, it is an honor to testify before you today on the activities of the United States Department of Homeland Security's Privacy Office, which I am privileged to lead as the first Chief Privacy Officer of the Department of Homeland Security.

The protection of privacy, of the dignity of the individual, is a value that is best embedded into the culture and structure of an organization and that is why I am so pleased to have been here from almost the very beginning. This value is one that must be embedded in the very culture and structure of the organization. I know that we can and will succeed in this—not only because our leadership believes in protecting the sanctity of the individual, but also because our over 180,000 employees are also great Americans, who believe in and act on these values—for themselves, their neighbors, and their children—each day.

**Establishment of the DHS Privacy Office**

The creation of the Department of Homeland Security and its many programs raise no shortage of important privacy and civil liberties issues for this nation to address. This Department, led by Secretary Tom Ridge, and this Administration, led by President Bush, are committed to addressing these critical issues as they seek to strengthen our homeland. A crucial part of this commitment is support for the creation and the mission of the Privacy Office at the Department of Homeland Security. Secretary Ridge articulated his vision for this office, stating that the privacy office “will be involved from the very beginning with every policy initiative and every program initiative that we consider,” to ensure that our strategy and our actions are consistent with not only the federal privacy safeguards already on the books, but also “with the individual rights and civil liberties protected by our laws and our Constitution.”

As Members of this subcommittee are uniquely aware, the enabling statute for the Department of Homeland Security contains Section 222, which directs the Secretary to appoint a senior official in the Department to assume primary responsibility for privacy policy. This includes conducting and oversight of formal Privacy Impact Assessments to assure that “the use of technologies sustain, and do not erode, privacy protections relating to the use,

collection and disclosure of personal information.” Along with adhering to the requirements of the Electronic Government Act of 2002, this office also oversees the Department’s compliance with the Privacy Act of 1974, and has been given the authority to evaluate legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government. Uniquely and importantly, under the enabling statute, the DHS Chief Privacy Officer reports directly to Congress on the activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act, internal controls, and other matters.

### **Key Legal Frameworks enforced by the Privacy Office**

The primary legal framework included in the enabling statutory language for the DHS Privacy Office is, obviously, the federal Privacy Act of 1974. The Privacy Act, 5 U.S.C. § 552a, provides a code of fair information practices that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal agencies. Emanating from almost global concerns about the growing aggregation of personal information--partly due to new technologies like mainframe computers of that day--this law provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, through detailed "system of records" notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one’s own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records. The Privacy Act is our country’s articulation of Fair Information Principles, and, when used zealously, protects the information of our citizens and also provides substantial access rights to them.

Under the Freedom of Information Act, 5 U.S.C. § 552, the principle that persons have a profound and fundamental right to know what their government is doing is enforced on a daily basis. Almost any person at any time has the right to query a federal agency about documents and records. Our government and our agency are grounded on principles of openness and accountability, tempered, of course, by the need to preserve the confidentiality of sensitive personal, commercial, and governmental information. The Freedom of Information Act is the primary statute that attempts to balance these countervailing public concerns. A robust FOIA/PA program is a critical part

of any agency’s fundamental processes; it helps to provide assurance to the public that, in pursuing its mission, an agency will also pursue balanced policies of transparency and accountability while preserving personal privacy. The U.S. federal government will spend tens of millions of dollars processing and responding to FOIA requests next year, and thousands of federal workers will spend all or part of their day compiling responses to those requests. Our agency alone has over 300 staff members across the Department who work full or part-time on Privacy Act and FOIA issues.

This past fall, the Office of Management and Budget released its guidance under Section 208 of the E-Government Act of 2002—a law that mandates Privacy Impact Assessments for new technologies and data collections. This, really a third pillar of the privacy framework at the federal level reflects, once again, a growing reliance on technology to move data--both in government spaces and on the Internet. The E-Government Act of 2002 contains a landmark requirement for privacy impact assessments by federal government agencies. The provisions of the E-government Act set forth a comprehensive framework for considering privacy in the ordinary course of business of government--serving our citizens. The Act and underlying guidance synthesize a myriad of prior guidance on privacy practices and notices, and will assist privacy practitioners in prioritizing their efforts. In particular, the guidance provides helpful information on the content of privacy notices and topics for required disclosure.

Further, the act requires the parameters for privacy impact assessments. Although in use by some agencies already, generally privacy impact assessments are a new and important tool in the toolbelt of privacy practitioners across the federal government. These new requirements formalize an important principle: that data collection by the government should be scrutinized for its impact on the individual and that individual’s data...and ideally before that data collection is ever implemented. The process, the very exercise of such scrutiny, is a crucial step towards narrowly tailoring and focusing data collection towards the core missions of government. This practice should provide even greater awareness, both by those seeking to collect the data and those whose data is collected, of the impact on the individual and the purpose of the collection.

I am pleased to have been a small part of the discussions towards the development of guidance on privacy impact assessments. These new requirements set the bar high for privacy practitioners. These requirements also reflect, I believe, a growing sensitivity and awareness on the part of our citizens regarding personal data flows in the public and private

sectors. I believe that this guidance will allow federal agencies to respond to citizens' concerns about these activities and also to be current with, or perhaps even slightly ahead of, the evolution of privacy practices in the private sector.

Under the Privacy Act, in concert with the Freedom of Information Act and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them. A robust FOIA/PA program is imperative to provide the public with assurances that any information DHS collects is being maintained consistent with all legal and regulatory requirements.

### **Operationalizing Privacy Throughout the Department of Homeland Security**

#### *Best Practices through Management Leadership*

The DHS Privacy Office works to promote best practices with respect to privacy and infuse respectful information privacy principles and practices for all employees into the DHS culture. A major and substantial goal at the outset for my tenure is to 'operationalize' privacy awareness and best practices throughout DHS, working not only with Secretary Ridge and our senior policy leadership of the various agencies and directorates of the department, but also with our Privacy Act and FOIA teams, as well as operational staff across the Department.

#### *Consistent Policies and Education Efforts*

Through internal educational outreach and the establishment of internal clearance procedures, we are sensitizing DHS directorates and components to consider privacy whenever developing new programs or revising existing ones. We are reviewing new technologies to ensure that privacy protections are given primary consideration in the development and implementation of these new systems. Our headquarters staff has been reviewing all Privacy Impact Assessments being conducted throughout the Department. In this process, DHS professionals have become educated about the need to consider--and the framework for considering--the privacy impact of their technology decisions. We are reviewing Privacy Act systems notices before they are sent forward and ensuring that these notices create only those systems of records that are necessary to support our mission. We also guide DHS agencies in developing appropriate privacy policies for their programs and serve as a resource for any question that may arise concerning privacy, information collection or disclosure. We work closely with various DHS policy teams, the Office of the General Counsel, and the Chief Information Officers to ensure that the mission of the Privacy Office is

reflected in all DHS initiatives. And of course we also work in concert with the Department's Office for Civil Rights and Civil Liberties, which is the other statutorily mandated office at DHS Headquarters with an individual liberties focus. The DHS Privacy Office also works collaboratively with Privacy Office and Privacy Officers across the Administration to consult on best practices and policies for agency privacy offices.

#### *Integrated Privacy and Disclosure Mandates*

The work of the Privacy Office includes not only the statutory Privacy Act and Privacy Impact Assessment work, but also integrates Freedom of Information Act oversight for the Department. This additional responsibility was redelegated to the Privacy Office last summer by Secretary Ridge, in recognition of the close connection between privacy and disclosure laws, and the functional synergies of the work of our Privacy Act and FOIA specialists across the Department.

### **Transparency and Outreach to the Public**

The DHS Privacy Office also seeks to anticipate and satisfy public needs and expectations, by providing a crucial link between those outside DHS who are concerned about the privacy impact of the Department's initiatives, and those inside the Department who are diligently working to achieve the Department's mission. Our role is not only to inform, educate, and lead privacy practice within the Department, but also to serve as listeners and as a receptive audience to those outside the Department who have questions or concerns about the Department's operations. To that end, and my office have engaged in consistent and substantial outreach efforts to members of the advocacy community, industry representatives, other U.S. agencies, foreign governments, and most importantly, the American public, not only to inform and educate those constituencies, but also, even more importantly, to hear their concerns, to share those concerns with the Department's leadership, and to see that those concerns are addressed in our programs and in the development of our policies. Recent coverage of our privacy program, in particular our Privacy Impact Assessment, or PIA, of the US-VISIT program, demonstrated how information collection efforts, especially those employing new or unfamiliar technology, can be done in a privacy-sensitive way. Operationally, this particular PIA demonstrated an effective internal system where by staff from across the department worked together to create a document that was at once technologically detailed and also reader-friendly.

**Key Policy Challenges***The Use of Private Sector Data*

I can think of no more compelling public policy issue, particularly one that affects the privacy of our citizens and visitors to this country, than the sharing of personal information between the public and private sector. It is one that has been successfully—and less successfully—navigated by other agencies within the Federal government, and it is one that we examine and grapple with in programs within every single directorate and agency within the Department of Homeland Security almost every day.

It is the Privacy Office's role to facilitate this conversation about and this examination of the responsible uses of information by government agencies like DHS. That role sometimes requires us to encourage, and even force conversation between those who label themselves as being concerned only with privacy, and those who consider themselves all about security. I challenge those who feel the need to be one or the other. It is, in fact, possible, to achieve both responsible privacy practices and achieve the mission of the Department of Homeland Security. Issues of privacy and civil liberties are most successfully navigated when the necessary legal and policy protections are built in to the systems or programs from the very beginning—both in the intelligent use of technology, and in the responsible execution of programs. Further, clear rules—both in the private sector and in the public sector—are necessary to ensure that such information sharing is done in a legitimate, respectful, and limited fashion.

*International Cooperation*

A key focus of the Privacy Office's work has been to engage the data protection authorities internationally. Privacy professionals the world over share a common interest in assuring public trust in government operations by encouraging transparency, as well as respect for fair information principles such as collection limitation, purpose specification, use limitation, data quality, security safeguards, openness, participation, and accountability. Our office has participated in the meetings of the International Association of Data Protection and Privacy Commissioners, although the office is not recognized at this time as an accredited data protection authority. We have also worked cooperatively with data protection authorities, or DPAs, to enable cross-border dispute resolution of personal data issues. Our office is both a point of appeals for complaints about our various directorates' programs, and also a point of contact for our international counterparts, whether acting to communicate policy concerns or individual citizens' complaints.

**Balancing the Need for Transparency and the Need for Security in Operations**

Perhaps the most difficult issue in a law enforcement or counter-terrorism context is the need to afford transparency and access to information for individuals, while also safeguarding information that is essential to an ongoing investigation of some type. Our office seeks to assist the agency in achieving this balance in a number of ways. First, rules and procedures for accessing information must be clear, easily attainable by individuals, and easily understood. Second, the classification of information as sensitive or otherwise protected must be narrowly tailored and well grounded. Third, systems must be in place whereby individuals can be assisted in correcting information that may impact them in some way, even when that information is deemed protected. An example of this is the use of citizen advocates or ombudsmen, where by government employees who have security clearance or access to information act on behalf of individuals to correct misidentifications or incorrect information that is associated with an individual. In addition, these processes must be efficient and minimally burdensome on the individual, and must provide for an appeal or further redress process that is adequately independent to act zealously and fairly on behalf of the individual. These processes exist in certain places within our Department, and should be implemented where personal information is collected by the government and used in a way that impacts the individual. The DHS Privacy Office plays a role in performing that independent review and appeal process for our directorates and citizens.

**The Defense of the Privacy Act**

The DHS Privacy Office applauds the subcommittee for its interest in privacy issues, and even more, privacy practices across the federal government. We in government are often quick to point to private-sector lapses in privacy policy, and we should be equally vigilant about our own use of personal data. While the federal government benefits from the requirements of the Privacy Act of 1974, it is also true that new technologies have allowed data sharing in new and perhaps unexpected ways. The Privacy Impact Assessment requirements of the E-Government Act of 2002 recognizes these new technological challenges and seeks to provide reader-friendly information about such data collections in a new and perhaps more technologically savvy fashion.

The Defense of Privacy Act shares many similarities with the PIA requirements under the E-Government Act, ones that are worth noting, such as the need for a "senior agency official with primary



responsibility for privacy policy.” While the need for a statutory privacy officer at DHS may be almost unique in the federal government, given the agency’s size and the co-mingling of parts of more than 22 former federal agencies, the need for senior policy leadership at any agency that affects public data is certainly recognized.

Further, the Act does clarify the timing of PIAs, to be both a prospective document, issued at the NPRM stage, and a final document, issued in response to public comments. We at DHS have, and fully intend to continue to publish PIAs for public comment and we believe that this public dialogue is essential to our understanding of public concerns about DHS programs.

### **Internal and External Role**

I am often asked whether I view my job as a privacy advocate and thus at odds with the activities of the Department. The answer is absolutely not. As Secretary Ridge has articulated on many occasions, the Department of Homeland Security’s mission is more than just counter-terrorism, more than just the protection of people and places and things. It is also the protection of our liberties and our way of life, and that includes the ability to engage in public life with dignity, autonomy, and a general expectation of respect for personal privacy. Thus, the protection of privacy is neither an adjunct nor the antithesis to the mission of the Department of Homeland Security. Privacy protection, in fact, is at the core of that mission.

I am very much in agreement with the statutory definition of my office's position as being both "within" and "without" the Department of Homeland Security. As part of the department, we are able to serve as educators, as leaders, and as full participants in the policy direction of important programs. And as outsiders, we are able to turn a critical eye on the most controversial and the most mundane aspects of the Department's operations. But I do not position my office as the enemy of the mission of this department. Rather, I see it as crucial, fundamental to successfully achieving that mission.

On a daily basis, I am aware of what it means to set parameters for the federal government’s use of personal information—information that has been given to us in our capacity as the provider of services, as the caretaker of the public’s physical security, and, most importantly, the custodian of the public’s trust. Secretary Ridge has said that “Fear of government abuse of information...is understandable, but we cannot let it stop us from doing what is right and responsible.” The antidote to fear, as he has said, “is an open, fair, and transparent process that guarantees the protection and the privacy of that data.” I commit to this Committee, to the American people whom we serve, and to our neighbors around the globe, that the Privacy Office is implementing this philosophy on a daily basis at the Department of Homeland Security.

I thank you for your time, and for your interest in and support of the Department of Homeland Security Privacy Office.



# **US-VISIT Program, Increment 1 Privacy Impact Assessment**

**December 18, 2003**

## **Contact Point**

**Steve Yonkers  
US-VISIT Privacy Officer  
Department of Homeland Security  
(202) 298-5200**

## **Reviewing Official**

**Nuala O'Connor Kelly  
Chief Privacy Officer  
Department of Homeland Security  
(202) 772-9848**

# US-VISIT Program, Increment 1

## Privacy Impact Assessment

### 1. Introduction

Congress has directed the Executive Branch to establish an integrated entry and exit data system to accomplish the following goals:<sup>1</sup>

1. Record the entry into and exit out of the United States of covered individuals;
2. Verify the identity of covered individuals; and
3. Confirm compliance by visitors with the terms of their admission into the United States.

The Department of Homeland Security (DHS) proposes to comply with this congressional mandate by establishing the United States Visitor and Immigration Status Indicator Technology (US-VISIT) program. The first phase of US-VISIT, referred to as Increment 1, will capture entry and exit information about non-immigrant visitors whose records are not subject to the Privacy Act. Rather than establishing a new information system, DHS will integrate and enhance the capabilities of existing systems to capture this data. In an effort to make the program transparent, as well as to address any privacy concerns that may arise as a result of the program, DHS's Chief Privacy Officer has directed that this PIA be performed in accordance with the guidance issued by OMB on September 26, 2003. As US-VISIT is further developed and deployed, this PIA will be updated to reflect future increments.

### 2. System Overview

- **What information is to be collected**

Individuals subject to the data collection requirements and processes of Increment 1 of the US-VISIT program (“covered individuals”) are nonimmigrant visa holders traveling through air and sea ports. The DHS regulations and related Federal Register notice for US-VISIT Increment 1 will fully detail coverage of the program.

The information to be collected from these individuals includes complete name, date of birth, gender, country of citizenship, passport number and country of issuance, country of residence, travel document type (e.g., visa), number, date and country of issuance, complete U.S. address, arrival and departure information, and for the first time, a photograph, and fingerprints. US-VISIT will capture and store this information from existing systems that already record it or are being modified to allow for its collection.

---

<sup>1</sup> Congress enacted several statutory provisions concerning an entry exit program, including provisions in: The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA) Public Law 106-215; The Visa Waiver Permanent Program Act of 2000 (VWPPA); Public Law 106-396; The U.S.A. PATRIOT Act, Public Law 107-56; and The Enhanced Border Security and Visa Entry Reform Act (“Border Security Act”), Public Law 107-173.

### • **Why the information is being collected**

In numerous statutes, Congress has indicated that an entry exit program must be put in place to verify the identity of covered individuals who enter or leave the United States. In keeping with this expression of congressional intent and in furtherance of the mission of the Department of Homeland Security, the purposes of US-VISIT are to identify individuals who may pose a threat to the security of the United States, who may have violated the terms of their admission to the United States, or who may be wanted for the commission of a crime in the U.S. or elsewhere, while at the same time facilitating legitimate travel.

### • **What opportunities individuals will have to decline to provide information or to consent to particular uses of the information and how individuals grant consent**

The admission into the United States of an individual subject to US-VISIT requirements will be contingent upon submission of the information required by US-VISIT, including biometric identifiers. A covered individual who declines to provide biometrics is inadmissible to the United States, unless a discretionary waiver is granted under section 212(d)(3) of the Immigration and Nationality Act. Such an individual may withdraw his or her application for admission, or be subject to removal proceedings. US-VISIT has its own privacy officer, however, to ensure that the privacy of all visitors is respected and to respond to individual concerns which may be raised about the collection of the required information. Further, the DHS Chief Privacy Officer will exercise comprehensive oversight of all phases of the program to ensure that privacy concerns are respected throughout implementation. The DHS Chief Privacy Officer will also serve as the review authority for all individual complaints and concerns about the program.

## **3. Increment 1 System Architecture**

US-VISIT Increment 1 will accomplish its goals primarily through the integration and modification of the capabilities of three existing systems:

1. The Arrival and Departure Information System (ADIS)
2. The Passenger Processing Component of the Treasury Enforcement Communications System (TECS)<sup>2</sup>
3. Automated Biometric Identification System (IDENT)

US-VISIT Increment 1 will also involve modification and extension of client software on Port of Entry (POE) workstations and the development of departure kiosks.

The changes to these systems include:

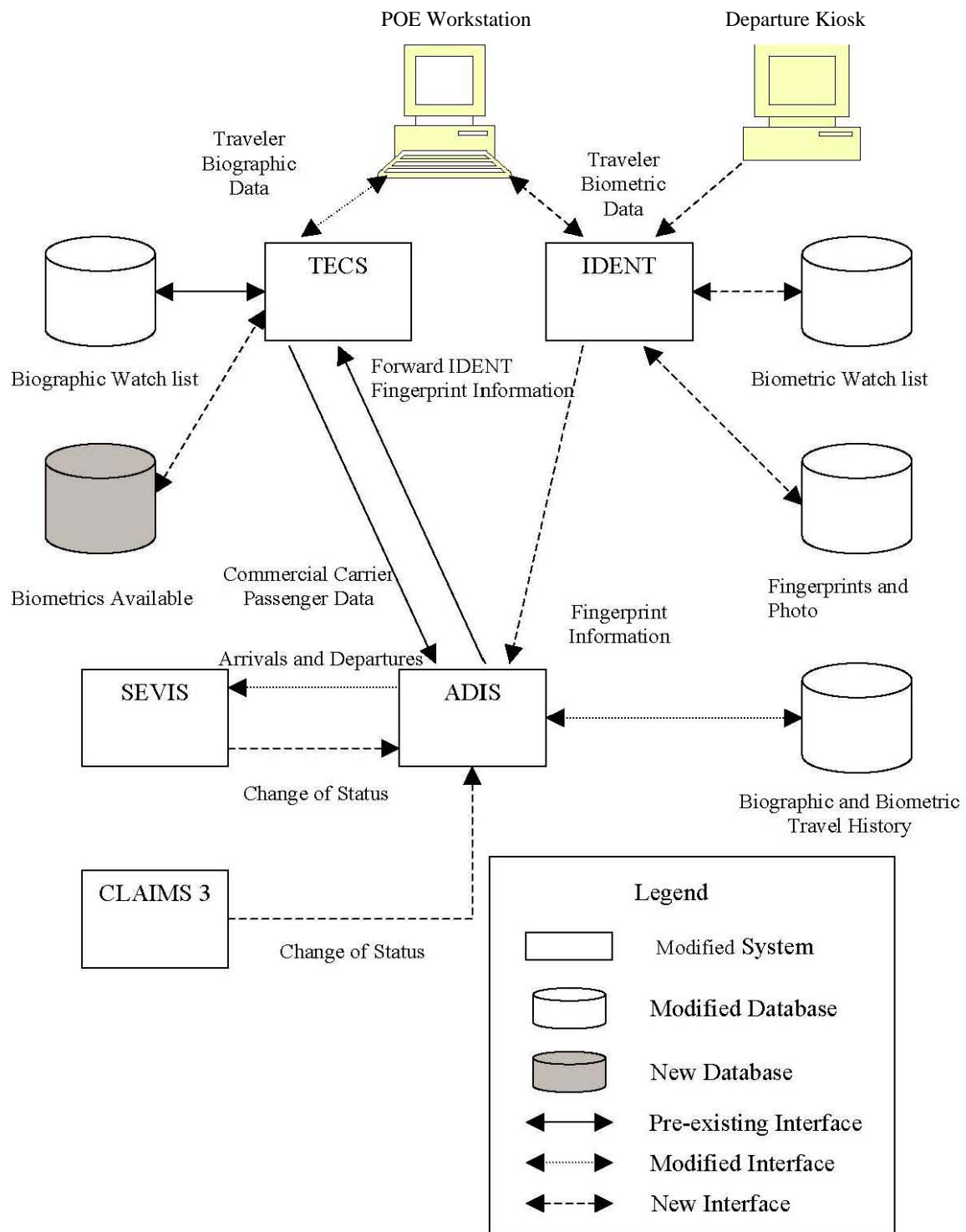
---

<sup>2</sup> As indicated in the US-VISIT Increment 1 Functional Requirements Document (FRD), the Passenger Processing Component of TECS consists of two systems, where “system” is used in the sense of the E-Government Act, title 44, Chapter 35, section 3502 of US Code; i.e., “a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.” The two systems, and the process relevant to US-VISIT Increment 1 that they support, are (1) Interagency Border Inspection System (IBIS), supporting the lookout process and providing interfaces with the Interpol and National Crime Information Center (NCIC) databases; and (2) Advance Passenger Information System (APIS), supporting the entry process by receiving airline passenger manifest information.

1. Modifications of TECS to give immigration inspectors the ability to display non-immigrant-visa (NIV) data.
2. Modifications to the ADIS database to accommodate additional data fields, to interface with other systems, and to generate various types of reports based on the stored data.
3. Modifications to the IDENT database to capture biometrics at the primary port of entry (POE) and to facilitate identity verification.
4. Establishment of interfaces to facilitate the transfer of biometric information from IDENT to ADIS and from ADIS to TECS.
5. Establishment of other interfaces to facilitate transfer of changes in the status of individuals from two other data bases—the Student and Exchange Visitor Information System (SEVIS) and the Computer Linked Application Information Management System (CLAIMS 3) to ADIS.

Figure 1 presents data flows in the context of the high-level system architecture.

Source: US-VISIT Increment 1 Functional Requirements Document



- **Intended use of the information**

DHS intends to use the information collected and maintained by US-VISIT Increment 1 to carry out its national security, law enforcement, immigration control, and other functions. Through the enhancement and integration of existing database systems, DHS will be able to ensure the entry of legitimate visitors, identify, investigate, apprehend and/or remove aliens unlawfully entering or present in the United States beyond the lawful limitations of their visit, and prevent the entry of inadmissible aliens. US-VISIT thus will enable DHS to protect U.S. borders and national security by maintaining improved immigration control. US-VISIT will also help prevent aliens from obtaining benefits to which they are not entitled.

#### **4. Maintenance and Administrative Controls on Access to the Data**

- **With whom the information will be shared**

The personal information collected and maintained by US-VISIT Increment 1 will be accessed principally by employees of DHS components—Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, and the Transportation Security Administration—and by consular officers of the Department of State. Additionally, the information may be shared with other law enforcement agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement intelligence information (whether civil or criminal) and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. The system of records notices for the existing systems on which US-VISIT draws provide notice as to the conditions of disclosure and routine uses for the information collected by US-VISIT, provided that any disclosure is compatible with the purpose for which the information was collected.

US-VISIT transactions will have a unique identifier to differentiate them from other IDENT transactions. This will allow for improved oversight and audit capabilities to ensure that the data are being handled consistent with all applicable federal laws and regulations regarding privacy and data integrity.

- **How the information will be secured**

The US-VISIT program will secure information and the systems on which that information resides, by complying with the requirements of the DHS IT Security Program Handbook. This handbook establishes a comprehensive program, consistent with federal law and policy, to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, and application rules, which will be applied to component systems, communications between component systems, and at interfaces between component systems and external systems.

One aspect of the DHS comprehensive program to provide information security involves the establishment of rules of behavior for each major application, including US-VISIT. These rules of behavior require users to be adequately trained regarding the security of their systems. These rules also require a periodic assessment of technical, administrative and managerial controls to enhance data integrity and accountability. System users must sign statements acknowledging that they have been trained and understand the security aspects of their systems. In addition, the

rules of behavior already in effect for each of the component systems on which US-VISIT draws will be applied to the program, adding an additional layer of security protection.

The table below provides detail on the various measures employed to address potential security threats to US-VISIT Increment 1.

### Security Threats and Mitigation Methods Detailed

Nature of Threat	Architectural Placement	Safeguard	Mechanism
Intentional physical threats from unauthorized external entities	ADIS	Physical protection	The ADIS database and application is maintained at a Department of Justice Data Center. Physical controls of that facility (e.g., guards, locks) apply and prevent entrée by unauthorized entities.
Intentional physical threats from unauthorized external entities	Passenger Processing Component of TECS	Physical protection	The Passenger Processing Component of TECS is maintained on a mainframe by CBP. Physical controls of the TECS facility (e.g., guards, locks) apply and prevent entrée by unauthorized entities.
Intentional physical threats from external entities	IDENT	Physical protection	IDENT is maintained on an IBM cluster. Physical controls of the facility (e.g., guards, locks) apply and prevent entrée by unauthorized entities.
Intentional physical threats from external entities	POE Workstation	Physical protection	Physical controls will be specific to each POE.
Intentional and unintentional electronic threats from authorized (internal and external) entities	System-wide	Technical protection: Identification and authentication (I&A)	User identifier and password, managed by the Password Issuance Control System (PICS).

## 5. Information Life Cycle and Privacy Impacts

The following analysis is structured according to the information life cycle. For each life-cycle stage—collection, use and disclosure, processing, and retention and destruction—key issues are assessed, privacy risks identified, and mitigation measures discussed. Risks are related to fair information principles—notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress—that form the basis of many statutes and codes.

### • Collection

US-VISIT Increment 1 collects only the personal information necessary for its purposes. While Increment 1 does not constitute a new system of records, it does expand the types of data held in its component systems to include biometric identifiers. By definition this creates a general privacy risk. This risk is mitigated, however, by establishment of a privacy policy supported and enforced by a comprehensive privacy program. This program includes a separate Privacy Officer for US-VISIT, mandatory privacy training for system operators, and appropriate safeguards for data handling.



## • Use and Disclosure

The IDENT and TECS systems collect data that are used for purposes other than US-VISIT. As a result, data collected for US-VISIT through these systems may become available for another functionality embodied in these component systems. This presents a potential notice risk: will the data be used for a purpose consistent with US-VISIT? This risk is mitigated in several ways. First, US-VISIT isolates US-VISIT data from non US-VISIT data on component systems, and users will be subject to specific privacy and security training for this data. Second, the IDENT and TECS systems already have their own published SORNs, which explain the uses to which the data they collect will be put, for US-VISIT as well as non-US-VISIT purposes. This, too, mitigates the notice risk. Third, Memoranda of Understanding and of Agreement are being negotiated with third parties (including other agencies) that will address protection and use of US-VISIT data, again to mitigate this notice risk.

## • Processing

Data exchange, which will take place over an encrypted network between US-VISIT Increment 1 component systems and/or applications is limited, and confined only to those that are functionally necessary. Although much of the personal information going into ADIS from SEVIS and CLAIMS 3 is duplicative of data entering ADIS from TECS, this duplication is to ensure that changes in status received from SEVIS or CLAIMS 3 are associated with the correct individual, even in cases of data element mismatches (i.e., differing values for the same data element received from different sources). This mitigates the data integrity risk. A failure to match generates an exception report that prompts action to resolve the issue. This also mitigates integrity risk by guarding against incorrect enforcement actions resulting from lost immigration status changes. (The data flows from SEVIS and CLAIMS 3 principally support changes in status.)

On the other hand, if a match is made, but there are some data element mismatches, no report is generated identifying the relevant records and data elements (one or more of which must have inaccurate or improper values) and no corrective action is taken. This is due to the resources that would be required to investigate all such events. This integrity risk again creates a possibility of incorrect enforcement actions if the match was made in error as a result of the data element mismatches. However, this aspect of the integrity risk is mitigated by subjecting all status changes that would result in enforcement actions to manual analysis and verification. A quality assurance process will also be used to identify any problem trends in the matching process.

## • Retention and Destruction

The policies of individual component systems, as stated in their SORNs, govern the retention of personal information collected by US-VISIT. Because the component systems were created at different times for different purposes, there are inconsistencies across the SORNs with respect to data retention policies. There is also some duplication in the types of data collected by each system. These inconsistencies and duplication result in some heightened degree of risk with respect to integrity/security of the data, and to access and redress principles, because personal information could persist on one or more component systems beyond its period of use or disappear from one or more component systems while still in use. These risks are mitigated, however, by having a Privacy Officer for US-VISIT to handle specific issues that

may arise, by providing review of the Privacy Officer’s decision by the DHS Chief Privacy Officer, and, to the extent permitted by existing law, regulations, and policy, by allowing covered individuals access to their information and permitting them to challenge its completeness. Additionally, as an overarching mechanism to ensure appropriate privacy protections, US-VISIT operators will conduct periodic strategic reviews of the data to ensure that what is collected is limited to that which is necessary for US-VISIT purposes.

US-VISIT Increment 1 will store fingerprint images, both in the IDENT database and transiently on the some POE workstations and departure kiosks. These images are, of course, sensitive, and their storage could present a security as well as a privacy risk. Because retention of fingerprint images is functionally necessary so that manual comparison of fingerprints can be performed to verify biometric watch list matches, appropriate mitigation strategies will be utilized, including encryption on the departure kiosks and physical and logical access controls on the POE workstations and on the IDENT system.

The chart below shows, in tabular form, the privacy risks associated with US-VISIT, Increment One, and the mitigation efforts that will address these risks.

**Privacy Threats and Mitigation Methods Detailed**

Type of Threat	Description of Threat	Type of Measures to Counter/Mitigate Threat
Unintentional threats from insiders <sup>3</sup>	Unintentional threats include flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians (i.e., personnel of organizations with custody of the information). These threats can be physical (e.g., leaving documents in plain view) or electronic in nature. These threats can result in insiders being granted access to information for which they are not authorized or not consistent with their responsibilities.	These threats are addressed by (a) developing a privacy policy consistent with Fair Information Practices, laws, regulations, and OMB guidance; (b) defining appropriate functional and interface requirements; developing, integrating, and configuring the system in accordance with those requirements and best security practices; and testing and validating the system against those requirements; and (c) providing clear operating instructions and training to users and system administrators.
Intentional threat from insiders	Threat actions can be characterized as improper use of authorized capabilities (e.g., browsing, removing information from trash) and circumvention of controls to take unauthorized actions (e.g., removing data from a workstation that has been not been shut off).	These threats are addressed by a combination of technical safeguards (e.g., access control, auditing, and anomaly detection) and administrative safeguards (e.g., procedures, training).

<sup>3</sup> Here, the term “insider” is intended to include individuals acting under the authority of the system owner or program manager. These include users, system administrators, maintenance personnel, and others authorized for physical access to system components.

<p>Intentional and unintentional threats from authorized external entities<sup>4</sup></p>	<p>Intentional: Threat actions can be characterized as improper use of authorized capabilities (e.g., misuse of information provided by US-VISIT) and circumvention of controls to take unauthorized actions (e.g., unauthorized access to systems).</p> <p>Unintentional: Flaws in privacy policy definition; mistakes in information system design, development, integration, configuration, and operation; and errors made by custodians</p>	<p>These threats are addressed by technical safeguards (in particular, boundary controls such as firewalls) and administrative safeguards in the form of routine use agreements which require external entities (a) to conform with the rules of behavior and (b) to provide safeguards consistent with, or more stringent than, those of the system or program.</p>
<p>Intentional threats from external unauthorized entities</p>	<p>Threat actions can be characterized by mechanism: physical attack (e.g., theft of equipment), electronic attack (e.g., hacking, interception of communications), and personnel attack (e.g., social engineering).</p>	<p>These threats are addressed by physical safeguards, boundary controls at external interfaces, technical safeguards (e.g., identification and authentication, encrypted communications), and clear operating instructions and training for users and system administrators.</p>

## 6. Summary and Conclusions

Legislation both before and after the events of September 11, 2001 led to the development of the US-VISIT Program. The program is based on Congressional concerns with visa overstays, the number of illegal foreign nationals in the country, and overall border security issues. Requirements for the program, including the implementation of an integrated and interoperable border and immigration management system, are embedded in various provisions of The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA) Public Law 106-215; The Visa Waiver Permanent Program Act of 2000 (VWPPA); Public Law 106-396; The U.S.A. PATRIOT Act, Public Law 107-56; and The Enhanced Border Security and Visa Entry Reform Act (“Border Security Act”), Public Law 107-173. As a result, many of the characteristics of US-VISIT were pre-determined. These characteristics include:

- Use of a National Institute of Standards and Technology (NIST) biometric standard for identifying foreign nationals;
- Use of biometric identifiers in travel and entry documents issued to foreign nationals, including the ability to read such documents at U.S. ports of entry;
- Integration of arrival/departure data on foreign nationals, including commercial carrier passenger manifests; and
- Integration with other law enforcement and security systems.

---

<sup>4</sup> These include individuals and systems which are not under the authority of the system owner or program manager, but are authorized to receive information from, provide information to, or interface electronically with the system.

These and other requirements substantially constrained the high-level design choices available to the US-VISIT Program. A major choice for the program concerned whether to develop an entirely or largely new system or to build upon existing systems. Given the legislatively imposed deadline of December 31, 2003 for establishing an initial operating capability, along with the various integration requirements, the program opted to leverage existing systems—IDENT, ADIS, and the Passenger Processing Component of TECS.

As a result of this choice for Increment 1, DHS has determined that a new information system would not be created. Nevertheless, in order to effectively and accurately assess the privacy risks of US-VISIT, and because the program represents a new business process, this Privacy Impact Assessment was performed. In the process of conducting this PIA, DHS identified the need to (1) update the SORNs of the ADIS and IDENT systems to accurately reflect US-VISIT requirements and usage, which has been accomplished, and (2) examine the privacy and security aspects of the existing SORNs and implement any additional necessary strategies to ensure the privacy and security of US-VISIT data.

Based on this analysis, it can be concluded that

- Most of the high-level design choices for US-VISIT Increment 1 were statutorily pre-determined;
- US-VISIT Increment 1 creates a pool of individuals whose personal information is at risk; but
- US-VISIT Increment 1 mitigates specific privacy risks; and
- US-VISIT, through its own Privacy Officer and in collaboration with the DHS Chief Privacy Officer, will continue to track, assess, and address privacy issues throughout the life of the US-VISIT program and update this PIA to reflect additional increments of the program.

### **Contact Point and Reviewing Official**

Contact Point: Steve Yonkers  
US-VISIT Privacy Officer  
(202) 298-5200

Reviewing Official: Nuala O'Connor Kelly  
Chief Privacy Officer, DHS  
(202) 772-9848

### **Comments**

We welcome your comments on this privacy impact assessment. Please write to: Privacy Office, Attn.: US-VISIT PIA, U.S. Department Of Homeland Security, Washington, DC 20528, or email [privacy@dhs.gov](mailto:privacy@dhs.gov). Please include US-VISIT PIA in the subject line of the email.

## Appendix

### US-VISIT Program

#### Privacy Policy

#### **What is the purpose of the US-VISIT program?**

The United States Visitor Immigrant Status Indicator Technology (US-VISIT) is a United States Department of Homeland Security (DHS) program that enhances the country's entry and exit system. It enables the United States to record the entry into and exit out of the United States of foreign nationals requiring a visa to travel to the U.S., creates a secure travel record, and confirms their compliance with the terms of their admission.

The US-VISIT program's goals are to:

- a. Enhance the security of American citizens, permanent residents, and visitors
- b. Facilitate legitimate travel and trade
- c. Ensure the integrity of the immigration system
- d. Safeguard the personal privacy of visitors

The US-VISIT initiative involves collecting biographic and travel information and biometric identifiers (fingerprints and a digital photograph) from covered individuals to assist border officers in making admissibility decisions. The identity of covered individuals will be verified upon their arrival and departure.

#### **Who is affected by the program?**

Individuals subject to the requirements and processes of the US-VISIT program ("covered individuals") are those who are not U.S. citizens at the time of entry or exit or are U.S. citizens who have not identified themselves as such at the time of entry or exit. Non-U.S. citizens who later become U.S. citizens will no longer be covered by US-VISIT, but the information about them collected by US-VISIT while they were non-citizens will be retained, as will information collected about citizens who did not identify themselves as such.

#### **What information is collected?**

The US-VISIT program collects biographic, travel, travel document, and biometric information (photographs and fingerprints) pertaining to covered individuals. No personally identifiable information is collected other than that which is necessary and relevant for the purposes of the US-VISIT program.

#### **How is the information used?**

The information that US-VISIT collects is used to verify the identity of covered individuals when entering or leaving the U.S. This enables U.S. authorities to more effectively identify covered individuals that:

- Are known to pose a threat or are suspected of posing a threat to the security of the United States;
- Have violated the terms of their admission to the United States; or
- Are wanted for commission of a criminal act in the United States or elsewhere.

Personal information collected by US-VISIT will be used only for the purposes for which it was collected, unless other uses are specifically authorized or mandated by law.

### **Who will have access to the information?**

Personal information collected by US-VISIT will be principally accessed by Customs and Border Protection, Immigration and Customs Enforcement, Citizenship and Immigration Services, and Transportation Security Officers of the Department of Homeland Security and Consular Officers of the Department of State. Others to whom this information may be made available include appropriate federal, state, local, or foreign government agencies when needed by these organizations to carry out their law enforcement responsibilities.

### **How will the information be protected?**

Personal information will be kept secure and confidential and will not be discussed with, nor disclosed to, any person within or outside the US-VISIT program other than as authorized by law and in the performance of official duties. Careful safeguards, including appropriate security controls, will ensure that the data is not used or accessed improperly. In addition, the DHS Chief Privacy Officer will review pertinent aspects of the program to ensure that proper safeguards are in place. Roles and responsibilities of DHS employees, system owners and managers, and third parties who manage or access information in the US-VISIT program include:

#### **1. DHS Employees**

As users of US-VISIT systems and records, DHS employees shall:

- Access records containing personal information only when the information is needed to carry out their official duties.
- Disclose personal information only for legitimate business purposes and in accordance with applicable laws, regulations, and US-VISIT policies and procedures.

#### **2. US-VISIT System Owners/Managers**

System Owners/Managers shall:

- Follow applicable laws, regulations, and US-VISIT program and DHS policies and procedures in the development, implementation, and operation of information systems under their control.
- Conduct a risk assessment to identify privacy risks and determine the appropriate security controls to protect against the risk.
- Ensure that only personal information that is necessary and relevant for legally mandated or authorized purposes is collected.
- Ensure that all business processes that contain personal information have an approved Privacy Impact Assessment. Privacy Impact Assessments will meet appropriate OMB

and DHS guidance and will be updated as the system progresses through its development stages.

- Ensure that all personal information is protected and disposed of in accordance with applicable laws, regulations, and US-VISIT program and DHS policies and procedures.
- Use personal information collected only for the purposes for which it was collected, unless other purposes are explicitly mandated or authorized by law.
- Establish and maintain appropriate administrative, technical, and physical security safeguards to protect personal information.

### **3. Third Parties**

Third parties shall:

- Follow the same privacy protection guidance as DHS employees.

#### **How long is information retained?**

Personal information collected by US-VISIT will be retained and destroyed in accordance with applicable legal and regulatory requirements.

#### **Who to contact for more information about the US-VISIT program**

Individuals whose personal information is collected and used by the US-VISIT program may, to the extent permitted by law, examine their information and request correction of inaccuracies. Individuals who believe US-VISIT holds inaccurate information about them, or who have questions or concerns relating to personal information and US-VISIT, should contact the Privacy Officer, US-VISIT Program, Department of Homeland Security, Washington, DC 20528. Further information on the US-VISIT program is also available at [www.dhs.gov/us-visit](http://www.dhs.gov/us-visit).

**ADDRESSES:** Please address your comments to the Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528. You must identify the docket number DHS/TSA-2003-1 at the beginning of your comments, and you should submit two copies of your comments. You may also submit comments via e-mail at [privacy@dhs.gov](mailto:privacy@dhs.gov). Please reference the docket number DHS/TSA-2003-1 in the subject line of the e-mail. If you wish to receive confirmation that DHS received your comments, please include a self-addressed, stamped postcard. DHS will make the comments available online at <http://www.dhs.gov>.

**FOR FURTHER INFORMATION CONTACT:** Privacy Office, Department of Homeland Security, Washington, DC 20528. Phone: 202-282-8000. Fax: 202-772-9738.

**SUPPLEMENTARY INFORMATION:**

**Background**

While still a part of the Department of Transportation, in January 2003, the Transportation Security Administration (TSA) proposed establishing a new system of records under the Privacy Act, known as "Aviation Security Screening Records." TSA intends to use this system of records to facilitate TSA's passenger and aviation security screening program under the Aviation and Transportation Security Act. TSA intends to use the CAPPS II system to conduct risk assessments to ensure passenger and aviation security.

Prior to March 1, TSA was an operating administration within the Department of Transportation (DOT). While part of the DOT, TSA published for public comment proposed system of records DOT/TSA 010. See 68 FR 2101 and 2002, Jan. 15, 2003. On March 1, 2003, TSA became a component of the Department of Homeland Security (DHS) and is now continuing work towards the system of records DHS/TSA 010.

Substantial comments were received in response to the prior Privacy Act notice. Those comments can be reviewed online at <http://dms.dot.gov/>, by entering the docket number "1437" under "Simple Search." Significant changes have been made to date to the proposed CAPPS II system in light of these comments, and the comments and concerns raised will continue to be considered during the testing and evaluation periods. Accordingly, we are publishing an Interim Final Notice of System of Records, modified to address public comment thus far, which is effective for and applicable to the internal test activity described herein. With the publication of this notice,

**DEPARTMENT OF HOMELAND SECURITY**

**Transportation Security Administration**

[Docket No. DHS/TSA-2003-1]

**Privacy Act of 1974: System of Records**

**AGENCY:** Transportation Security Administration (TSA), Department of Homeland Security (DHS).

**ACTION:** Notice of status of system of records; Interim final notice; Request for further comments.

**SUMMARY:** The Transportation Security Administration (TSA) proposed in January 2003 to establish a new system of records under the Privacy Act, known as "Passenger and Aviation Security Screening Records." This system of records would be established primarily to support the development of a new version of the Computer Assisted Passenger Prescreening System, or "CAPPS II." This notice is to inform the public that substantial comments were received in response to the prior Privacy Act notice (68 FR 2101, January 15, 2003); that significant changes have been made to date to the proposed CAPPS II system and to the CAPPS II Privacy Act notice in light of these comments; that limited developmental technical testing will occur with test data, including personal information on U.S. persons available from commercial databases, including those within and affiliated with the travel industry; and that concerns raised will continue to be considered during the testing and evaluation periods. Additional comments are sought on the modifications made to this Privacy Act notice. A further Privacy Act notice will be published in advance of any active implementation of the CAPPS II system.

**DATES:** This notice is effective on August 1, 2003. Comments due on September 30, 2003.



internal systems testing will begin, using this System of Records.

The CAPPS II system is still under consideration and development and certain elements of the technological systems are proposed for testing with attention to the issues raised in the comments received, particularly the accuracy, efficiency, and privacy impact of the proposed CAPPS II system. Results of the current technological tests, as well as the comments received, will inform the design of the final CAPPS II system. A further Privacy Act notice will be published in advance of any active implementation of the CAPPS II system for real-time passenger screening.

#### Proposed CAPPS II System

TSA is establishing this system of records, now entitled "Passenger and Aviation Security Screening Records," to support the function of TSA's CAPPS II system. CAPPS II is intended to conduct risk assessments and authentications for passengers traveling by air to, from or within the United States.

#### *Sources of Information Contained in the CAPPS II System; Process Flow*

Under the proposed CAPPS II system, TSA will obtain electronically, either from airlines or from Global Distribution Systems, a passenger's "passenger name record" (PNR) as collected from the passenger by a reservation system. PNR includes the routine information collected at the time a passenger makes a flight reservation. A PNR may include each passenger's full name, home address, home telephone number, and date of birth, as well as some information about that passenger's itinerary. No additional information beyond this data is required to be collected from passengers for the operation of CAPPS II.

The CAPPS II system will access PNRs prior to the departure of the passenger's flight. Selected information will be securely transmitted to commercial data providers, for the sole purpose of authenticating passenger identity. This authentication will be accomplished not by a permanent comingling of data, but merely by the commercial data providers transmitting back to TSA a numeric score, which is an indication of the percentage of accuracy of the match between the commercial data and the data held by TSA. This will enable TSA to have a reasonable degree of confidence that each passenger is who he or she claims to be. TSA recognizes that inaccuracies in the commercial data may exist and that the CAPPS II system must allow for

and compensate for such inaccuracies; this test phase is intended to test and further develop such capabilities in the system.

Commercial data providers will receive a limited amount of identifying information from TSA with regard to each passenger, and will provide TSA with an authentication score and code indicating a confidence level in that passenger's identity. The commercial data providers will not provide TSA with any additional information about the individual. They will not acquire ownership of the data, nor will they be permitted to retain the data in any commercially usable form. TSA will not permit the commercial data providers to use this data for any purpose other than in connection with the CAPPS II program. Importantly, the commercial data provider will not retain information about the response they provide to TSA in any record about the individual that they maintain. Further, no persistent link between an individual's records in the private sector and that person's records within the CAPPS II system will be created.

Once CAPPS II has authenticated a passenger's identity, it will conduct its risk assessment. The risk assessment function is conducted internally within the U.S. government and will determine the likelihood that a passenger is a known terrorist, or has identifiable links to known terrorists or terrorist organizations. National security information from within the Federal Government, as well as information reflecting Federal officials with high levels of security clearance, will be part of this analysis function.

After the CAPPS II system becomes operational, it is contemplated that information regarding persons with outstanding state or Federal arrest warrants for crimes of violence may also be analyzed and applied in the context of this system. At or after such time as the system becomes operational, where there is an indication of a serious violation of criminal law (as described in the Routine Use section, below), such information may be shared between law enforcement agencies and the Department of Homeland Security and appropriate action may be taken. It is further anticipated that CAPPS II will be linked with the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program at such time as both programs become fully operational, in order that the processes at both border and airport points of entry and exit are consistent. Any such linkages will be performed in full compliance with the Privacy Act of 1974, including any

applicable requirement for additional notice.

It is important to note the CAPPS II system is designed to determine the likelihood that a passenger is a known terrorist, or has identifiable links to known terrorists or terrorist organizations, including both foreign and domestic terrorist organizations.

Lastly, it is anticipated that dynamic inputs to the system from intelligence sources will allow the system to respond to current threat conditions and information on a timely basis.

#### *Impact on Traveling Public*

Based upon the combination of information derived from commercial sources, national security sources, and dynamic intelligence data, each traveling passenger will be identified with a "risk score," indicating whether that person's information leads to a determination of low, high, or unknown risk to passenger and aviation security.

In the vast majority of cases, passengers will be identified as "low risk," and will simply pass through the ordinary airport security screening process to their flights.

In a small percentage of cases, passengers may be found to present an elevated, uncertain or "unknown risk" of terrorism. In such cases, the passengers in question will be subjected to heightened security screening prior to boarding their flights. Once these passengers have successfully completed this screening, they will proceed to their flights in the normal manner; they will not be penalized, nor will additional information about them be retained within the CAPPS II system.

Where a passenger is found to be "high risk"—to have identifiable links to terrorism, law enforcement or other appropriate authorities will be notified for appropriate action. It is anticipated that the number of passengers so identified as high risk will be extremely small, but any so identified may be critically significant in the context of homeland security.

#### *Privacy Practices*

The Department of Homeland Security is committed to working with airlines and the travel industry to provide greater understanding and awareness of the purposes for and the scope of CAPPS II. Consistent with fair information principles, the Department of Homeland Security will work towards adequate notice to the passenger when that passenger provides information that will be used for security purposes.

Further, DHS is committed to providing access to the information that

is contained in the CAPPS II system to the greatest extent feasible consistent with national security concerns. As detailed below, passengers can request a copy of most information contained about them in the system from the CAPPS II passenger advocate. Further, DHS is currently developing a robust review and appeals process, to include the DHS privacy office.

#### System Testing of CAPPS II

At this point, partly in response to concerns raised by the public about the viability and function of the CAPPS II program, TSA plans to test certain portions of the system, including the technological communications between the CAPPS II system and the various data sources, as well as the identity authentication programs. These tests are intended to respond to public concerns about speed, accuracy, and efficiency of the system. Testing will be concerned with the accuracy of public and private information contained in the system, particularly in the authentication process; the speed of response of the system; identifying and minimizing the data necessary to effectively conduct the operation of CAPPS II; and the overall ability of the system to identify risk levels effectively. During these tests, TSA will use and retain PNR data for the duration of the test period. It is anticipated that the test duration may be as long as 180 days. A persistent link to law enforcement databases will not be created for the purposes of the test, nor will data from the test be transmitted to airport screeners or used for screening purposes during the test period. If, however, an indication of terrorist or potential terrorist activity is revealed during the test period, appropriate action will be taken. A final Privacy Act notice will be published before the CAPPS II system is deployed.

#### Public Comments

TSA received well over 200 comments on proposed system of records DOT/TSA 010—"Aviation Security Screening Records." Comments generally expressed concern that the proposed CAPPS II system was too broad in scope and would prove invasive to passengers' privacy. Several commenters stated that the proposed system of records contained too wide a variety of personal information and allowed for the collection and retention of too much information on private citizens. Commenters also expressed concern about the quality of data contained in commercial databases, and that such data could be used to prevent them from traveling by air. Some commenters stated that the proposed

retention of data for up to 50 years was too long. Another concern expressed was the broad variety of "routine uses," which, in the opinion of some commenters, allowed TSA far too much discretion to disseminate private information. One commenter expressed the view that the CAPPS II system would lead to the misallocation of security resources.

TSA respects the concerns raised by commenters and has modified the proposed system of records to address many of those concerns. The test of the technological systems responds, in part, to concerns of accuracy, efficiency, and effectiveness, which are among the underpinnings of evaluating such a system's impact on an individual's privacy. Any subsequent modifications to the system that arise from the knowledge gained from these tests will be published in a subsequent notice.

This system notice reduces the extent to which TSA will maintain or disseminate personal information on airline passengers. At the same time, however, TSA must ensure that it collects information sufficient to carry out its security screening functions in an efficient and effective manner, consistent with its legislative mandate to ensure passenger and aviation security. In establishing the parameters of the Passenger and Aviation Security Screening Records system, TSA has attempted to address privacy interests of passengers and the public, while simultaneously working towards increased transportation security.

#### Responses to Comments: Modifications to System

As discussed above, several commenters objected to the amount of personal information that TSA proposed to maintain in the proposed system of records. Under this system notice, TSA will not retain significant amounts of personal information after completion of a passenger's itinerary. TSA eliminated language in the proposed notice that could be read to mean that TSA will collect and maintain large amounts of information about individuals.

Concerns have been raised about the retention of data after a passenger's travel. In response, TSA is working to minimize the length of time any data about passengers will be retained. In response to concerns, the proposal to maintain information about certain individuals for up to 50 years has been deleted. Under the final CAPPS II program, when active, it is anticipated that TSA will delete all records of travel for U.S. citizens and lawful permanent resident aliens not more than a certain number of days after the safe

completion of their travel itinerary. At this time, the amount of information about non-U.S. persons and the length of time for which that information will be kept when the CAPPS II system is deployed are matters still under consideration.

The limited test data used during the test period will be retained solely for the duration of the test; at the conclusion of the test, DHS expects that all data from the test will be destroyed, unless otherwise required by law. In either case, such data will not be included in the live activation of CAPPS II.

Commenters also objected to the broad description of the types of data to be collected from passengers. Specifically, commenters stated that there was no clear explanation of what TSA meant by "associated data" in the reference to TSA's collection of PNR and "associated data." In response, TSA has deleted the phrase "associated data."

Some commenters objected to the large variety of different types of data that TSA proposed to maintain in the system of records. TSA has significantly reduced the variety of data to be maintained in the system. For the vast majority of passengers, the CAPPS II system, when active, will maintain only the routine information that all individuals provide when making reservations, as contained in the PNR, including full name, date of birth, home address and home phone number, to the extent available. In addition, the CAPPS II system will contain authentication scores and codes, and a TSA-generated risk assessment score. The system will also contain some information derived from governmental databases containing information on, or pertinent to, the detection of terrorists and their associates and the detection of the serious criminal violations detailed in this notice, as well as information on government officials and other persons holding security clearances or positions of trust such as not to warrant heightened scrutiny. However, in response to specific concerns regarding the use of information about an individual's creditworthiness or individual health records, TSA will not use measures of creditworthiness, such as FICO scores, and individual health records in the CAPPS II traveler risk determination.

Other commenters raised concerns that large numbers of people would be prevented from flying as a result of the use of inaccurate commercial records. One of TSA's primary purposes in creating this new system is to avoid the kind of miscommunication and improper identification that has, on

45268

Federal Register / Vol. 68, No. 148 / Friday, August 1, 2003 / Notices

occasion, occurred under the systems currently in use. During the test period, TSA hopes to confirm that the use of the CAPPS II program will significantly reduce improper identification.

#### Routine Uses

In response to the comments received that expressed concerns about the further dissemination of passenger information, TSA has narrowed several routine uses in the proposed notice, and eliminated others in their entirety, as follows:

Proposed Routine Use 1 (to Federal, State, local, international, or foreign agencies) (now Routine Use 1) has been narrowed to pertain to specified violations of criminal law.

Proposed Routine Use 3 (now Routine Use 3) has been modified to specify immigration and intelligence agencies.

Proposed Routine Uses 4 (to individuals and organizations), 5 (to government agencies in connection with employment, contract or benefit matters) and 6 (to news media) have been deleted.

Proposed Routine Use 2 (now Routine Use 2) and proposed Routine Use 9 (now Routine Use 4) have been modified slightly to make the language consistent with the routine uses in other TSA systems of records. These changes are not substantive and do not expand or narrow the scope of the routine uses.

Proposed Routine Use 10 (now Routine Use 5) has been modified slightly to allow for disclosures to airports and aircraft operators only to the extent required in the interests of counterterrorism or passenger or aviation security.

Proposed Routine Use 11 (now Routine Use 6) has been modified to permit disclosure to the General Services Administration (GSA), in addition to the National Archives and Records Administration (NARA), for purposes of records management inspections. Both GSA and NARA have the statutory authority under 44 U.S.C. 2904 and 2906 to conduct inspections or surveys of TSA records, which was not reflected in the proposed routine use. This modification corrects the omission.

#### DHS/TSA 010

##### SYSTEM NAME:

Passenger and Aviation Security Screening Records.

##### SECURITY CLASSIFICATION:

Classified, sensitive.

##### SYSTEM LOCATION:

Records are maintained at the Transportation Security Administration (TSA), Department of Homeland

Security, P.O. Box 597, Annapolis Junction, MD 20701-0597.

##### CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals traveling to, from or within the United States by passenger air transportation; known terrorists and individuals on terrorism watch lists; persons with outstanding federal or state warrants for crimes of violence; government officials or other persons holding requisite security clearances, positions of trust and confidence, or otherwise deemed not to require heightened scrutiny.

##### CATEGORIES OF RECORDS IN THE SYSTEM:

(a) Passenger Name Records (PNRs) obtained from airlines, Global Distribution Systems and Computer Reservation Systems (the specific contents of PNRs often vary by airline, but will include at least the following passenger information: Full name, date of birth, home phone number, home address, and travel itinerary); other information in PNR may include payment information, and frequent flier number (if any);

(b) Authentication scores and codes obtained from commercial data providers;

(c) Numerical "risk scores" generated by the CAPPS II system;

(d) Watch lists and government databases containing information on known terrorists and terrorist associates, or other information pertinent to the detection of terrorists and their associates, or pertinent to the detection of outstanding state or federal warrants for crimes of violence.

(e) Names of and other identifying information about government officials or other persons holding security clearance or positions of trust and confidence, such as not to warrant heightened scrutiny.

##### AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

49 U.S.C. 114, 44901, and 44903.

##### PURPOSE(S):

The system will be used to facilitate the development, testing, and conduct of the Computer Assisted Passenger Prescreening System II (CAPPS II). The purpose of CAPPS II is to minimize threats to passenger and aviation security by determining which passengers should be afforded additional scrutiny prior to boarding an aircraft. In addition, CAPPS II is designed to determine the likelihood that a passenger is a known terrorist, or has identifiable links to known terrorists or terrorist organizations, including both foreign and domestic terrorist

organizations, or otherwise poses a threat to passenger or aviation security.

##### ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

(1) To appropriate Federal, State, local, international, or foreign agencies or authorities responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, or order, or in accordance with law or international agreements, where DHS becomes aware of an outstanding state or federal arrest warrant for a crime of violence.

(2) To contractors, grantees, experts, or consultants when necessary to perform a function or service related to the CAPPS II system or this system of records for which they have been engaged. Such recipients are required to comply with the Privacy Act, 5 U.S.C. 552a, as amended.

(3) To Federal, State, local, international, or foreign agencies or authorities, including those concerned with law enforcement, visas and immigration, and to agencies in the Intelligence Community, or in accordance with law or international agreements, with respect to persons who may pose a risk of air piracy or terrorism or who may pose a threat to aviation, passenger safety or national security.

(4) To the Department of Justice or other Federal agencies conducting litigation, or in a proceeding before a court, adjudicative or administrative body, when: (a) TSA, or (b) any employee of TSA in his/her official capacity, or (c) any employee of TSA in his/her individual capacity where DOJ or TSA has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to litigation or has an interest in such litigation, and TSA determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which TSA collected the records.

(5) To airports and aircraft operators, only to the extent the disclosure is deemed required for counterterrorism or passenger or aviation security purposes.

(6) To the General Services Administration and the National Archives and Records Administration (NARA) in records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

##### DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:****STORAGE:**

Records are stored electronically at a TSA secure facility. The records are stored on magnetic disc, tape, digital media, CD-ROM, and may also be retained in hard copy format in secure file folders.

**RETRIEVABILITY:**

Data are retrievable by the individual's name or other identifier, as well as non-identifying information, such as flight number.

**SAFEGUARDS:**

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable DHS automated systems security and access policies. The computer system from which records could be accessed is policy and security based, meaning access is limited to those individuals who require it to perform their official duties. The system also maintains a real-time auditing function of individuals who access the system. Classified information is appropriately stored in a secured facility, and secured databases and containers and in accordance with other applicable requirements, including those pertaining to classified information.

**RETENTION AND DISPOSAL:**

A request is pending for NARA approval for the retention and disposal of records in this system. For U.S. persons, (*i.e.*, citizens and lawful permanent resident aliens), records will be deleted within a set number of days after the safe completion of the travel to which the record relates. The duration of data retention for other persons is still under consideration. Factors to be considered in determining data retention for those persons will include the extent of information required to accurately authenticate passenger identity and the amount of data available from commercial data on non-U.S. persons, relative to U.S. persons. Existing records obtained from other government agencies, including intelligence information, watch lists, and other data, will be retained for three years, or until superseded.

Passenger data used for purposes of system development and testing will be deleted upon completion of the test phase.

**SYSTEM MANAGER(S) AND ADDRESS:**

Director, CAPPs II, TSA, PO Box 597, Annapolis Junction, MD 20701-0597.

**NOTIFICATION PROCEDURES:**

Pursuant to 5 U.S.C. 552a(k), this system of records may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual.

**RECORD ACCESS PROCEDURES:**

Although the system is exempt from record access procedures pursuant to 5 U.S.C. 552a(k), DHS has determined that all persons may request access to records containing information they provided by sending a written request to the CAPPs II Passenger Advocate (P.O. Box 597, Annapolis Junction, MD 20701-0597). To the greatest extent possible and consistent with national security requirements, such access will be granted. In the case of air passengers, this data is contained in the PNR. Individuals requesting access must comply with the Department of Homeland Security Privacy Act regulations on verification of identity (6 CFR 5.21(d)). Individuals must submit their full name, current address, and date and place of birth. You must sign your request and your signature must either be notarized or submitted by you under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. As noted above, however, in order to protect passenger privacy, PNR data is not retained for any significant time in this system. Accordingly, in most cases, the response to a record access request will very likely be that no record of the passenger exists in the system.

**CONTESTING RECORD PROCEDURES:**

A passenger who, having accessed his or her records in this system, wishes to contest or seek amendment of those records should direct a written request to the CAPPs II Passenger Advocate, at P.O. Box 597, Annapolis Junction, MD, 20701-0597. The request should include the requestor's full name, current address and date of birth, as well as a copy of the record in question, and a detailed explanation of the change sought. If the matter cannot be resolved by the CAPPs II Passenger Advocate, further appeal for resolution may be made to the DHS Privacy Office. While non-U.S. persons are not covered by the Privacy Act, such persons will still be afforded the same access and redress remedies. These remedies for all persons will more fully detailed in the CAPPs II privacy policy, which will be published before the system becomes fully operational.

**RECORD SOURCE CATEGORIES:**

Pursuant to 5 U.S.C. 552a(k), this system is exempt from publishing the categories of sources of records.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

Portions of this system are exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) pursuant to 5 U.S.C. 552a(k)(1) and (k)(2).

Issued in Washington, DC, on July 22, 2003.

**Tom Ridge,**

*Secretary, U.S. Department of Homeland Security.*

[FR Doc. 03-19574 Filed 7-31-03; 8:45 am]

BILLING CODE 4910-62-P



# Homeland Security

## Department of Homeland Security Privacy Office

### Report to the Public on Events Surrounding jetBlue Data Transfer

#### *Findings and Recommendations<sup>1</sup>*

February 20, 2004

#### *Summary*

A potential privacy violation involving the Transportation Security Administration (“TSA”) (at the time, a division of the Department of Transportation, now a component of the Department of Homeland Security), was brought to the attention of this office in September 2003. The potential privacy violation involved the transfer of Passenger Name Records (“PNR”) from jetBlue Airways to the Department of Defense, a transfer that occurred with some involvement by TSA personnel. While the incidents in question occurred during 2001 and 2002, preceding the creation of the Department of Homeland Security, the matter raises serious concerns about the proper handling of personally identifiable information by government employees now within the Department of Homeland Security. Accordingly, the Privacy Office conducted an investigation of the facts surrounding the transfer of data.

#### *Background*

The Department of Homeland Security Privacy Office was established in April 2003, pursuant to Section 222 of the Homeland Security Act, which requires the

---

<sup>1</sup> The Understanding of Facts and the Findings and Recommendations of this report will remain open for a period of 30 days following the publication of this Report, in order to provide a means of due process to participants who may wish to offer further clarifications, corrections, or otherwise augment the record reviewed by the DHS Privacy Office. If no new material information comes to light within that time, this report shall be deemed final in its current form.

Secretary to “appoint a senior official to assume primary responsibility for privacy policy.”<sup>2</sup>

In the course of fulfilling the privacy policy and complaint resolution mandates of Section 222, the DHS Privacy Office receives and responds to complaints and inquiries from Members of Congress, representatives of advocacy organizations, representatives of foreign governments, and the citizens of the United States regarding the operations of the many components of the Department of Homeland Security.

The discovery in September 2003 of a potential privacy violation involving jetBlue Airways (“jetBlue”), the Department of Defense (“DOD”), and, possibly, the Transportation Security Administration, led to numerous inquiries to the DHS Privacy Office from individual members of the public, representatives of advocacy organizations, offices of Members of Congress, and the press, regarding involvement by TSA employees. The incidents in question took place during 2001 and 2002, when TSA was part of the Department of Transportation. However, as of March 1, 2003, the TSA is part of the Department of Homeland Security (“DHS” or “the Department”).

Accordingly, the DHS Privacy Office responded to these inquiries with a statement that the DHS Privacy Office would investigate and report on any findings regarding possible involvement by TSA, now-DHS employees in these events. Following is that report.

### *Methodology*

This report is not intended to comment on allegations involving jetBlue’s activities or the activities of Department of Defense employees or contractors, which in these circumstances is beyond the statutory purview of the DHS Privacy Office.<sup>3</sup>

---

<sup>2</sup> Such responsibility includes:

- (1) Assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
- (2) Assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- (3) Evaluating legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the Federal Government;
- (4) Conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected; and
- (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.

Homeland Security Act, Section 222; 6 U.S.C.A. § 142 (2003).

<sup>3</sup> The Findings and Recommendations take into account, however, the important role that the DHS Privacy Office should assume in leading discussions about, and the development of, best practices for data sharing

This report reflects the DHS Privacy Office's understanding of the events of 2001 and 2002 concerning the transfer of PNR from jetBlue Airways to the Department of Defense, based on reasonable efforts by the Privacy Office to determine the nature of these events as of February 20, 2004, and lays out specific recommendations, particularly concerning DHS policy on sharing personal data. Should further information come to light regarding these events, this report may be amended and its conclusions altered.

This report is based on a substantial document review by the DHS Privacy Office. These documents were obtained from a variety of sources: documents voluntarily provided by DHS employees and other Federal employees and civilians, documents requested from TSA by the DHS Privacy Office, documents provided by airline representatives and companies involved in these events, and public documents available on the Internet and elsewhere. The DHS Privacy Office thanks the TSA Administrator, the Deputy Administrator, and their staffs, for their assistance in obtaining necessary documents. The DHS Privacy Office further recognizes the work of our colleagues at the TSA FOIA office for their assistance in compiling documents for our review.

The DHS Privacy Office further performed interviews with Department of Homeland Security employees, Department of Defense employees, Department of Defense contractors, jetBlue officials, other persons involved in these events, and citizens who claimed unique knowledge of the events.

This report is based entirely on information culled from these documents and interviews, and to the extent possible, independently verified by other persons with knowledge of these events.

### *Understanding of Facts*

In the fall of 2001, following the horrific events of September 11, 2001, numerous private companies that designed or promoted novel technologies approached various Federal agencies with offers of assistance in the national response to these events and in waging the War on Terrorism. As the Department of Homeland Security did not yet exist, these offers of assistance were fielded by numerous other federal agencies with a nexus to defense, technology, commerce, or counter-terrorism.

One such offer was made by Torch Concepts of Huntsville, Alabama. Representatives of Torch Concepts approached the Department of Defense with an unsolicited proposal involving data pattern analysis, geared towards enhancing the security of military installations throughout the country and, possibly, internationally. To simplify, the proposal suggested that through analysis of personal characteristics of persons who sought access to military installations, the users of such a program might be able to predict which persons posed a risk to the security of that installation. This project

---

between the private and public sectors, particularly in the use of technologies that can have a substantial effect on the privacy of personal information about an individual.

arose out of a desire to prevent attacks on military installation, following the attack on the Pentagon.

Because DOD was interested in this proposal – which subsequently became known as the Base Security Enhancement Program--in March 2002, Torch Concepts was added as a subcontractor to an existing contract with SRS Inc., for the purpose of performing a limited initial test of this technology. A subordinate task order for the contract included a reference to using “P&R”—an erroneous reference to PNR, or passenger name records, as a possible data source for the test.

This reference to “P&R data” suggests that while Torch Concepts developed the idea and method for data analysis, their proposal depended on an outside source of data for operational completeness. Indeed, in seeking to perform testing of their concept, Torch Concepts sought access to a large, national-level database to be used in assessing the efficacy of their data analysis tool for assessing terrorist behavior. During late 2001 and early 2002, Torch Concepts apparently approached a number of federal agencies that operated national government databases containing personal information that Torch believed might be appropriate. These requests did not yield any data. Torch then sought other commercial sources of national characteristics, and began contacting data aggregators and airlines, as it was apparently believed that national airline passenger databases would contain adequate cross-sections of personal characteristics, and that airline passenger lists might yield appropriate analytical information. There are conflicting reports regarding whether the test would simply seek a cross-section of data, whether the test was directly aimed at analyzing information regarding airline passengers traveling within close proximity of a military installation, or whether the test reflected a more equal interest in base and airline security.

Torch Concepts, according to public documents, approached both American Airlines and Delta Airlines, but again their requests were rejected. Torch then sought assistance from Capitol Hill, entreating Members of Congress to intervene on their behalf with airlines or the federal agencies. At the same time, Torch was told by representatives of one or more airlines that the airlines would not engage in such sharing unless the Department of Transportation and/or TSA was consulted and approved of such data sharing.

In April 2002, Torch Concepts contacted the Department of Transportation (“DOT”), and a number of meetings followed during May and June, including meetings with representatives of the DOT Office of Congressional Affairs and several DOT program offices, including offices at the TSA responsible for development of the second-generation Computer Assisted Passenger Prescreening System (“CAPPS II”), and representatives of the Chief Information Officer’s (“CIO”) office at the Department of Transportation. The TSA Congressional Affairs office was involved due to the Congressional requests. At the time of these meetings, the CAPPS II program was in the most preliminary stages of development, the creation of the program having been announced in March 2002.



In July and August 2002, conversations between DOT, DOD, and Torch Concepts continued. While these conversations reportedly did touch on the concurrent development of CAPPs II, the purpose of these conversations reportedly was not to assist in CAPPs II development, and TSA officials purportedly stated during these conversations that the development of these projects should remain separate. DOT officials appear to have recognized similarities in the large-scale pattern analysis technology between the proposed CAPPs II and the technology offered by Torch, but that while the technology was similar, it was not precisely what was anticipated for CAPPs II. Thus, while they were interested in the results of the testing, it was not performed for their benefit or the benefit of the CAPPs II program. DOT/TSA officials purportedly made it clear in these meetings that the Torch Concepts project was necessarily separate from CAPPs II development, given the sensitivity of the impending contracting process associated with that program.

As a result of these meetings, DOT/TSA officials agreed to assist the DOD-Torch project in obtaining the consent of an airline to share passenger data for the purposes of the Base Security Enhancement project. TSA officials contacted jetBlue Airways in New York, and began conversations with jetBlue regarding this project. TSA officials state that their understanding at this time was that the technology was intended to flag potential terrorists arriving by air in the areas near military bases. However, documents produced by DOD reflect a more general “base security” purpose. While one form of base security may have included preventing terrorist attacks by air directed at military installations, the overarching purpose was the prevention of unauthorized or unwanted entry onto military bases via a variety of forms of entry.

As a result of these conversations, on July 30, 2002, a relatively new employee of TSA sent jetBlue a written request that jetBlue provide archived passenger data to the Department of Defense for the Base Security Enhancement Program. This request does not appear to have been approved or directed by senior DOT officials. This request by TSA to jetBlue to retrieve personal records from its database and to share such data with DOD was significant, particularly as no airline had otherwise previously agreed to share data directly with DOD.

In August 2002, Torch Concepts was informed by Acxiom Corporation (“Acxiom”), a data aggregator serving as a contractor for jetBlue, that Torch would receive data from jetBlue; in September 2002, data was transferred from jetBlue to Torch Concepts. It is not clear the entire range of data elements that was included about each passenger, but, at a minimum, name, address, telephone, and some itinerary-related information was included. A total of five million records, representing over 1.5 million passengers, were transferred. The actual transfer of the data, was, in fact, accomplished between Acxiom (acting as a contractor for jetBlue) and Torch Concepts.<sup>4</sup> There does not appear to have been any fee paid by Torch Concepts for the transfer of the jetBlue passenger data. In October 2002, Torch Concepts separately purchased additional demographic data from the data aggregator, Acxiom.

---

<sup>4</sup> It should be noted that Acxiom later became a contractor for the CAPPs II program, but was not involved in CAPPs II at the time of this data transfer.

Torch Concepts documents reveal that the “five million P&R” (sic) records were inadequately diverse, as the passenger data on this airline represented only certain regions of the country and a limited flight pattern. The data is described in Torch Concepts document as “tourist-like passengers” with “limited origins and destinations,” and lacking “passenger travel history.” The demographics data purchased from Acxiom further revealed passenger name; gender; home specifics—whether a renter or owner; years at current residence; economic status/income; number of children; social security number; number of adults in household; occupation; and vehicles owned.

Torch Concepts used the Acxiom and jetBlue data to perform tests of the base security system. In doing so, Torch “de-identified” the data, or stripped it of name and other unique identifiers. According to Torch Concepts, all jetBlue data received for these tests were later destroyed, and hard drives containing any residual data were removed from use and given to legal counsel for safekeeping.

In spring 2003, Torch Concepts representatives appeared at a conference on homeland security technology in Alabama. This Southeastern Software Engineering Conference was sponsored by the National Defense Industrial Association (it has been incorrectly reported that this event was sponsored by the Department of Homeland Security). While the date on Torch Concepts’ PowerPoint presentation was February 25, 2003, Torch Concept representatives state that the conference actually occurred in April. The presentation given by Torch Concepts at the Southeastern Software Engineering Conference revealed information previously set forth in this Report, and also included a chart of “anomalous demographic information for one passenger.” This PowerPoint slide revealed, apparently without name, a number of addresses and social security numbers associated with one traveler. The concept for this presentation was entitled “Homeland Security Airline Passenger Risk Assessment.” The focus of this presentation was not the Base Enhancement project that was the initial purpose of the project, but rather, a process of analyzing passenger demographics for risk assessment. The presentation concluded that “several distinctive travel patterns were identified,” and that “demographic groupings appear common to each,” and that “known airline terrorists appear readily distinguishable from the normal jetBlue passenger patterns.” Further, the presentation stated that “if a more comprehensive P&R (sic) data base were available, it is expected that analysis could identify and characterize all normal travel patterns.”

It should be noted that DOD, TSA, jetBlue, and Acxiom do not appear to have been aware of this presentation at that time; the relevant parties neither participated in preparing the presentation, nor did they give their permission for the personal data disclosed in the Torch Concepts PowerPoint presentation. Of particular note, this presentation reveals that Torch Concepts believe it was “promised” the same data as was being used for CAPPs II. Upon clarification, Torch officials state that this comment meant that they understood they would receive PNR. Other parties to the conversations between DOT and Torch Concepts do not recall that any such promise relating to CAPPs II was made, particularly given the early stages of the CAPPs II program development at that time.

Almost a year after the data transfer, in the summer of 2003, DHS officials and others separately acknowledged that jetBlue had further agreed to test TSA's CAPPS II system. TSA employees had substantial communications with jetBlue, and a number of other airlines, throughout the development of the CAPPS II system. jetBlue, in particular, expressed an interest in participating in preliminary tests of this system for a variety of reasons, including a willingness to support homeland security efforts, given the impact of September 11, 2001, on their home base, New York. Further, jetBlue believed that its customer base was (and continues to be) disproportionately affected by the operation of the current CAPPS I system, which targets for secondary screening a number of behaviors which may be common to jetBlue customers.

During 2003, there were substantial delays in implementing testing of CAPPS II, including, not insignificantly, a realization by TSA employees during this period that the jetBlue privacy policy prevented such data sharing, and that jetBlue would need to take affirmative action to amend such policies before any testing began.

In late September 2003, members of the public, seeking to halt jetBlue's reported involvement in testing the CAPPS II system, engaged in substantial research regarding jetBlue's public activities. These parties were easily able to obtain the above-referenced PowerPoint presentation, which was available on the Internet at that time, and publicly alleged an improper data transfer to the Federal government of significant size and impact. In response, jetBlue Chief Executive Officer David Neeleman released a public statement that "Although I had no knowledge of this data transfer at the time it was made, I accept full responsibility for this action by our company." Further, Mr. Neeleman, while recognizing that the data transfer was a violation of the company's privacy policy, stated that "I can understand why the decision was made to comply with this request ... in the wake of the September 11 attacks, and as New York's hometown airline, all of us at jetBlue were very anxious to support our government's efforts to improve security." In response to this disclosure, jetBlue stated publicly that it would not engage in any testing of the TSA's CAPPS II program.

With these revelations, the DHS Privacy Office began its investigation. The DHS Privacy Office has been in contact with representatives of TSA, DOT, DOD/Department of the Army, jetBlue, Acxiom, Torch Concepts. The DHS Privacy Office has participated in meetings on Capitol Hill, and has been contacted by staff of Members of Congress interested in the investigation, as well as members of the advocacy community and the press. The DHS Privacy Office has kept the DHS Inspector General apprised only of the existence of this investigation, but not its findings, until shortly in advance of the publication of this report.

In addition to the above, it is important to note what was not found. There is no evidence that jetBlue or Acxiom provided data directly to TSA or DOT in connection with these events. On the contrary, numerous parties confirmed that the data was provided by jetBlue (through its contractor, Acxiom) to Torch Concepts. Further, there is no evidence that Torch Concepts or DOD shared results of this testing directly with

DOT/TSA, or that DOT/TSA officials had specific knowledge of the exact purpose for or scope of the testing that was to be performed. There is no evidence at this time that DOT/TSA facilitated the sharing of data for this project from any other airline or other source. There is also no evidence that any privacy policy or Privacy Act impact was discussed in the meetings between DOT, DOD, and Torch Concepts.

The DHS Privacy Office is aware that TSA, while part of DOT and also while part of DHS, separately sought data from several airlines for the purpose of testing CAPPS II, and, that while initially several airlines expressed interest in sharing data, these offers were later rescinded. At this time, there is no evidence that CAPPS II testing has taken place using passenger data.

### *Findings*

Although the events giving rise to the data transfer occurred in 2001 and 2002, prior to the establishment of the Department of Homeland Security, TSA, formerly within the Department of Transportation, is now a component of DHS. Accordingly, the Privacy Office devoted significant resources to examining this incident in an effort to understand precisely what occurred and why. Further, the Privacy Office will continue to devote significant attention to the establishment of internal controls and procedures to ensure that future activities of the department are guided by clear principles for the responsible use of personal information.

In connection with events that occurred in 2002 involving jetBlue, DOD, and TSA, the Department of Homeland Security Privacy Office finds that:

1. No Privacy Act violation by TSA employees occurred in connection with this incident. There is no evidence that any data were provided directly to TSA or its parent agency at the time, DOT. On the contrary, the evidence demonstrates that passenger data were transferred directly by jetBlue's contractor, Acxiom, to Torch Concepts. As a result, the Privacy Act of 1974, which regulates the Federal Government's collection and maintenance of personally identifiable data on citizens and legal permanent residents, does not appear to have been violated by TSA actions. Because TSA did not receive passenger data, no new system of records under the Privacy Act was established within TSA, nor was any individual's personal data used or disclosed by TSA, its employees or contractors, in violation of the Privacy Act.
2. The primary purpose for the data transfer was the "Base Security Enhancement Project." While the knowledge gained from testing the pattern analysis technology proposed for this project may have ultimately benefited other data analysis programs, including TSA's CAPPS II, such benefit was not the stated purpose of the base security enhancement project.

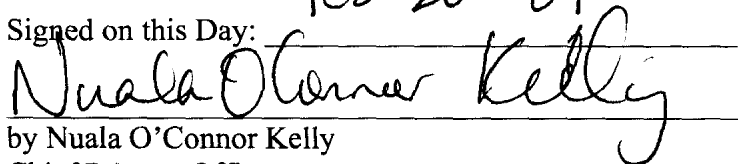
3. TSA employees were involved in the data transfer. Both documentary and verbal evidence indicate that TSA employees both facilitated contacts between the airline and DOD and failed to identify the privacy policy and privacy impact on individuals whose information might have been shared with the Department of Defense or its contractors.
4. TSA participation was essential to encourage the data transfer. As several airlines had refused to participate in this program absent TSA's involvement, it appears that, *but for* the involvement of a few TSA officials in these events, the data would likely not have been shared by jetBlue with the Department of Defense and its contractors.
5. The TSA employees involved acted without appropriate regard for individual privacy interests or the spirit of the Privacy Act of 1974. In doing so, it appears that their actions were outside normal processes to facilitate a data transfer, with the primary purpose of the transfer being other than transportation security. Such sharing exceeds the principle of the Privacy Act which limits data collection by an agency to such information as is necessary for a federal agency to carry out its own mission. While these actions may have been well intentioned and without malice, the employees arguably misused the oversight capacity of the TSA to encourage this data sharing.

### *Recommendations*

1. *Corrective Action.* The TSA employees involved, must, at a minimum, attend substantial Privacy Act and privacy policy training and must certify such training to the satisfaction of the DHS Privacy Office.
2. *Referral to the Inspector General.* It is beyond the scope of the Privacy Office to determine whether these employees may have otherwise exceeded the normal scope of TSA operations. The above findings will be referred to the Department of Homeland Security's Inspector General for further review. After reviewing the results of the Chief Privacy Officer's report and the Inspector General's report, if any, other remedial action may be recommended if appropriate.
3. *Comprehensive Privacy Training.* This incident underscores that additional and systematic training is needed. The DHS Privacy Office has been analyzing current training efforts in an attempt to formalize privacy education and training across the Department. This process will continue. The DHS Privacy Office also encourages each directorate or related agency, such as the TSA, to evaluate its systemic education and training programs for new and existing employees.

4. *Establishment of Guidelines for Data Sharing.* While existing Privacy Act processes require government contractors to abide by Privacy Act rules, this matter presents a somewhat new situation involving cooperative sharing of data between the private sector and the federal government for security purposes. The DHS Privacy Office has begun, and will continue to establish clear rules for voluntary and compulsory data sharing with private-sector entities. Such rules will include (1) adequate oversight of such data sharing by senior officials of DHS agencies; (2) adequate review of the controlling private-sector privacy policies and applicable laws; and (3) documented compliance with the Privacy Act of 1974, among other matters.

Signed on this Day:

Feb 20 '04  


by Nuala O'Connor Kelly  
Chief Privacy Officer

U.S. Department of Homeland Security

**DEPARTMENT OF HOMELAND SECURITY****Privacy Office; Data Integrity, Privacy, and Interoperability Advisory Committee****AGENCY:** Privacy Office, DHS.**ACTION:** Committee management; notice of establishment and request for applications for membership.**SUMMARY:** The Department of Homeland Security provides notice of establishment of the Data Integrity, Privacy, and Interoperability Advisory Committee. This notice also requests qualified individuals interested in serving on this committee to apply for membership.**DATES:** Applications forms for membership should reach the Privacy Office on or before April 30, 2004.**ADDRESSES:** You may request a copy of the Committee's charter or an application form by writing to Ms. Tina Hubbell, U.S. Department of Homeland Security Privacy Office, Washington, DC 20528, by calling (202) 772-9848, or by faxing (202) 772-5036. The Committee's charter will also be available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy). Send your application in written form to the above address.**FOR FURTHER INFORMATION CONTACT:** Ms. Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, telephone (202) 772-9848.**SUPPLEMENTARY INFORMATION:** The Secretary of the Department of Homeland Security has determined that the establishment of the Data Integrity, Privacy, and Interoperability Advisory Committee is necessary and in the public interest in connection with the performance of duties of the Chief Privacy Officer. This determination follows consultation with the Committee Management Secretariat, General Services Administration.*Name of Committee:* Data Integrity, Privacy, and Interoperability Advisory Committee.*Purpose and Objective:* The Committee will advise the Secretary of the Department of Homeland Security (DHS) and the Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues

within DHS that affect individual privacy, as well as data integrity and data interoperability and other privacy related issues.

*Duration:* Continuing.*Balanced Membership Plans:* This Committee will be composed of not less than 12 members, appointed by the Secretary, who shall be specially qualified to serve on the Committee by virtue of their education, training, or experience and who are recognized experts in the fields of data protection, privacy, interoperability, and/or emerging technologies. Membership shall be balanced among individuals from the following fields:

- Individuals who are currently working in the areas of higher education or research in public (except Federal) or not-for-profit institutions;
- Individuals currently working in non-governmental industry or commercial interests, including at least one representative of a small to medium enterprise;
- Other individuals, as determined appropriate by the Secretary.

Individuals may be required to have an appropriate security clearance before appointment to membership on the Committee.

Membership terms will be for up to 4 years, with the terms of the initial appointees staggered in 2-, 3-, and 4-year terms to permit continuity and orderly turnover of membership. Thereafter, members shall generally be appointed to 4-year terms of office.

Members will not be compensated for their service on the Committee; however, while attending meetings or otherwise engaged in Committee business, members may receive travel and per diem in accordance with Federal Government regulations.

Dated: April 6, 2004.

**Nuala O'Connor Kelly,**  
*Chief Privacy Officer.*

[FR Doc. 04-8106 Filed 4-8-04; 8:45 am]

BILLING CODE 4410-10-P

**Federal Register**

Vol.69, No. 85

Monday, My 3, 2004

Notices **24178****DEPARTMENT OF HOMELAND SECURITY****Data Integrity, Privacy, and Interoperability Advisory Committee****AGENCY:** Privacy Office, Department of Homeland Security.**ACTION:** Extension of application period for committee membership.**SUMMARY:** The period for candidates to submit applications for membership on the Data Integrity, Privacy, and Interoperability Advisory Committee is being extended to May 15, 2004.**DATES:** Application forms for membership should reach the Privacy Office on or before May 15, 2004.**ADDRESSES:** You may request an application form by writing to Tina Hubbell, U.S. Department of Homeland Security Privacy Office, Washington, DC 20528, by calling (202) 772-9848, or by faxing (202) 772-5036. Send your application in written form to the above address.*Responsible DHS Officials:* Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528, telephone (202) 772-9848.**SUPPLEMENTARY INFORMATION:** In an April 9, 2004, Federal Register Notice (69 FR 18923 April 9, 2004), the Department of Homeland Security provided notice that the Secretary was establishing the Data Integrity, Privacy, and Interoperability Advisory Committee and requested that qualified individuals interested in serving should apply for membership by April 30, 2004. Potential candidates have requested more time to submit applications. Therefore, we are extending the period to submit applications to May 15, 2004. Applications should be received on or before that date but will be accepted for a limited time after May 15.

Dated: April 28, 2004.

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

[FR Doc. 04-10057 Filed 4-30-04; 8:45 am]

BILLING CODE 4410-10-M



# Homeland Security

## **FREEDOM OF INFORMATION ACT ANNUAL REPORT** **FOR FISCAL YEAR 2003**

### CONTENTS

- I. Basic Information Regarding Report
  - II. How to Make a FOIA Request
  - III. Definition of Terms
  - IV. Exemption 3 Statutes
  - V. Initial FOIA/PA Access Requests
  - VI. Appeals of Initial Denials of FOIA/PA Requests
  - VII. Compliance with Time Limits/Status of Pending Requests
  - VIII. Comparisons with Previous Year(s)
  - IX. Costs/FOIA Staffing
  - X. Fees
  - XI. FOIA Regulations
-



**I. BASIC INFORMATION REGARDING REPORT**

This is the Fiscal Year 2003 Freedom of Information Act/Privacy Act (FOIA/PA) Report for the Department of the Homeland Security. The Department of Homeland Security was established on January 24, 2003; the twenty-two agencies that became part of this Department transferred to DHS as of March 1, 2003.

DHS consists of four new operating directorates: Science and Technology (S&T), Information Analysis and Infrastructure Protection (IAIP); Border and Transportation Security (BTS); and Emergency Preparedness and Response (EPR). The Directorates are listed in **bold** in the following charts. To the extent that these directorates processed FOIA requests this year, with the exception of the Office of the Inspector General, the work was done primarily by the DHS Privacy Office, which also handled FOIA requests for DHS Headquarters offices. EPR and BTS, however, encompass components that pre-existed the creation of DHS; these components have provided data on FOIA processing for compilation into this report. See FOIA Post: Annual Report Guidance for DHS-Related Agencies, posted at: <http://www.usdoj.gov/oip/foiapost/2003foiapost29.htm>. These components are signified in the following charts by the use of *italics*.

The United States Secret Service and the United States Coast have become operating units within DHS. Additionally, The immigration service functions of the former Immigration and Naturalization Service have been reorganized into a separate operating unit within DHS, now called United States Citizenship and Immigration Services (USCIS), and is signified by the use of **bold**. Preexisting INS Border Patrol and Inspections Programs have been combined with similar functions formerly performed by the United States Customs Service into a new component in BTS, Customs and Border Protection. Preexisting INS Investigations, Detention and Removal, and Intelligence functions have also been combined with similar functions formerly performed by the Customs Service into another BTS component, Immigration and Customs Enforcement. The Federal Protective Service, formerly part of the General Services Administration, is now part of BTS. These components are signified by the use of *italics*.

The Privacy Office prepared this report in collaboration with component FOIA Officers.

**If you have any questions about this report, you may direct them to:**

Elizabeth Withnell

Acting Departmental Disclosure Officer

Ph: 202-772-5015; Fax: 202-772-5036

**Address:**

Departmental Disclosure Officer

Department of Homeland Security

245 Murray Lane, SW, Building 410

Washington D.C. 20528

Department of Homeland Security FOIA Home Page:

<http://www.dhs.gov/dhspublic/display?theme=48>

Paper copies of this report may be obtained by contacting the Departmental Disclosure Officer. The report can also be downloaded from the DHS FOIA website.

**II.****A. Names, Addresses, and Contact Numbers for DHS FOIA Officers.****Privacy Office (PO)**

Elizabeth Withnell  
Ph: 202-772-5015  
Fax: 202-772-5036

**Address:**

Departmental Disclosure Officer  
Department of Homeland Security  
245 Murray Lane, SW, Bldg. 410  
Washington, D.C. 20528

**Federal Law Enforcement Training Center (FLETC)**

Billy J. Spears  
Ph: 912-267-3103  
Fax: 912-267-3113

**Address:**

1131 Chapel Crossing Road  
Glynco, GA 31524  
Attention: Disclosure Officer  
Building #: TH389-C

**Federal Emergency Management****Agency (FEMA)**

Eileen Leshan  
Ph: 202-646-4115; Fax: 202-646-4536

**Address:**

Office of General Counsel  
500 C Street, SW, Room 840  
Washington, DC 20472

**US Citizenship and Immigration Service (USCIS)**

Magda Ortiz  
Ph: 202-307-5701; Fax: 202-353-8166

**Address:**

425 I Street NW  
FOIA/PA Program  
ULLICO Bldg, 2<sup>nd</sup> Floor  
Washington, DC 20536

**United States Coast Guard (USCG)**

Commandant (CG-611)  
Ph: 202-267-6929; Fax: 202-267-4814

**Address:**

United States Coast Guard  
2100 Second Street, SW  
Washington, DC 20593

**Transportation Security Administration (TSA)**

Patricia M. Riep-Dice  
Ph: 571-227-2502; Fax: 571-227-1946

**Address:**

TSA Headquarters – East Tower, 4<sup>th</sup> Floor, TSA-20  
601 South 12<sup>th</sup> Street  
Arlington, VA 22202-4204

**United States Secret Service**

Latita Huff  
Ph: 202-406-5503; Fax: 202-406-5154

**Address:**

U. S. Secret Service  
950 H Street, NW  
Suite 3000  
Washington, DC 20223

**US Customs and Border Protection (CBP)**

Joanne Roman Stump  
Ph: 202-572-8717; Fax: 202-572-8727

**Address:**

U.S. Customs Service  
1300 Pennsylvania Avenue, NW  
Mint Annex  
Washington, DC 20229

**US Immigration & Customs Enforcement (ICE)**

Gloria L. Marshall  
Ph: 202-616-7489; Fax: 202-616-7612

**Address:**

Mission Support Division  
Office of Investigations  
U.S. Immigration & Customs Enforcement  
425 I Street, NW - Room 4038 (CAB Bldg.)  
Washington, DC 20536

**Federal Protective Service (FPS)**

Joseph Gerber  
Ph: 202-501-0265; Fax: 202-208-5866

**Address:**

Federal Protective Service  
1800 F Street, N.W., Suite 234  
Washington, D.C. 20405

**DHS Office of the Inspector General (OIG)**

Richard Reback  
Ph: 254-4100; Fax: 254-4285

**Address:**

Department of Homeland Security  
245 Murray Lane, SW, Bldg. 410  
Washington, D.C. 20528

**B.** A Brief Description of the Department Of Homeland Security's response-time ranges.

A breakdown of DHS response times by component is in Section VII of this report, "Compliance with Time Limits/Status of Pending Requests."

**C.** A Brief description of why some requests are not granted.

**The most common reasons reported by DHS components for not granting requests were: 1) the records were exempt from release under FOIA Exemption 6; 2) the records were exempt from release under FOIA Exemption 7C; and the records were exempt from release under FOIA Exemption 5.**

**III.** Definition of Terms.

**A.** Agency-Specific

1. PO Privacy Office
2. BTS Border and Transportation Security Directorate
3. EPR Emergency Preparedness and Response Directorate
4. S&T Science and Technology Directorate
5. IAIP Information Analysis and Infrastructure Protection Directorate
6. USCG United States Coast Guard
7. USSS United States Secret Service
8. USCIS United States Citizenship and Immigration Services
9. FLETC Federal Law Enforcement Training Center
10. CBP United States Customs and Border Protection
11. ICE Immigration and Customs Enforcement
12. TSA Transportation and Security Administration
13. FEMA Federal Emergency Management Agency
14. FPS Federal Protective Service
15. OIG Office of the Inspector General

**B.** Basic Terms Used in This Report

**1. FOIA/PA request** -- Freedom of Information Act/Privacy Act request. A FOIA request is generally a request or access to records concerning a third party, an organization, or a particular topic of interest. A Privacy Act request is a request for records concerning oneself; such requests are also treated as FOIA requests. (All requests for access to records, regardless of which law is cited by the requester, are included in this report.)

**2. Initial Request** -- a request to a federal agency for access to records under the Freedom of Information Act.

**3. Appeal** -- a request to a federal agency asking that it review at a higher administrative level a full denial or partial denial of access to records under the Freedom of Information Act, or any other FOIA determination such as a matter pertaining to fees.

**4. Processed Request or Appeal** -- a request or appeal for which an agency has taken a final action on the request or the appeal in all respects.

**5. Multi-track processing** – a system in which simple requests requiring relatively minimal review are placed in one processing track and more voluminous and complex requests are placed in one or more tracks. Requests in each track are processed on a first-in/first-out basis. A requester who has an urgent need for records may request expedited processing (see below).

**6. Expedited processing** -- an agency will process a FOIA request on an expedited basis when a requester has shown an exceptional need or urgency for the records which warrants prioritization of his or her request over other requests that were made earlier.

**7. Simple request** -- a FOIA request that an agency using multi-track processing places in its fastest (nonexpedited) track based on the volume and/or simplicity of records requested.

**8. Complex request** -- a FOIA request that an agency using multi-track processing places in a slower track based on the volume and/or complexity of records requested.

**9. Grant** -- an agency decision to disclose all records in full in response to a FOIA request.

**10. Partial grant** -- an agency decision to disclose a record in part in response to a FOIA request, deleting information determined to be exempt under one or more of the FOIA's exemptions: or a decision to disclose some records in their entirety, but to withhold others in whole or in part.

**11. Denial** -- an agency decision not to release any part of a record or records in response to a FOIA request because all the information in the requested records is determined by the agency to be exempt under one or more of the FOIA's exemptions, or for some procedural reason (such as because no record is located in response to a FOIA request).

**12. Time limits** -- the time period in the Freedom of Information Act for an agency to respond to a FOIA request (ordinarily 20 working days from proper receipt of a "perfected" FOIA request).

**13. "Perfected" request** -- a FOIA request for records which adequately describes the records sought, which has been received by the FOIA office of the agency or agency component in possession of the records, and for which there is no remaining question about the payment of applicable fees.

**14. Exemption 3 statute** -- a separate federal statute prohibiting the disclosure of a certain type of information and authorizing its withholding under FOIA subsection b) (3).

**15. Median number** -- the middle, not average, number. For example, of 3, 7, and 14, the median number is 7.

**16. Average number** -- the number obtained by dividing the sum of a group of numbers by the quantity of numbers in the group. For example, of 3, 7, and 14, the average number is 8.

**IV. Exemption 3 Statutes relied on by the Department during Fiscal Year 2003.**

<b>STATUTE</b>	<b>TYPE OF INFORMATION</b>	<b>CASE CITATION UPHELD BY COURTS.</b>
8 U.S.C. 1160(B)(6)	Information on Special Agricultural workers	None
8 U.S.C. 1304(B)	Registration of Aliens	None
8 U.S.C.A. 1186a(4)(C)	Confidentiality of Information Concerning Abused Alien Spouse or Child	None
18 U.S.C. 2510-2550	Intercepted Communications Wiretaps	Lam Lek Chong v. DEA, 929 F.2d 729 (D.C. Cir. 1991)
31 U.S.C. 5319	Records on Monetary Instruments and Transactions	Small v. IRS, 820 F. Supp. 163 (D.N.J. 1992)
41 U.S.C. 253b(m)	Prohibition on Release of Contractor Proposals	None
46 U.S.C. 7319	Records regarding issued merchant mariner documents	None
49 U.S.C. 114(s)	Nondisclosure of Security Activities	None
Rule 6(e) of the Federal Rules of Criminal Procedures	Grand Jury Information	Senate of P.R. v. United States Dep't of Justice, 823 F.2d 574 (D.C. Cir. 1987).

**V. Initial FOIA/PA Access Requests**

**A. Number of Initial Requests**

<b>Directorate</b>	<b>Number of Requests Pending at the End of Fiscal Year 2002</b>	<b>Number of Requests Received in Fiscal Year 2003</b>	<b>Number of Requests Processed in Fiscal Year 2003</b>	<b>Number of Requests Pending at the End of Fiscal Year 2003</b>
<b>PO</b>	N/A*	282	264	18
<b>OIG</b>	N/A*	19	6	13
<b>S&amp;T</b>	N/A*	0	0	0
<b>IAIP</b>	N/A*	0	0	0
<b>EPR</b>	N/A*	0	0	0
<i>FEMA</i>	250	438	438	250
<b>USCG</b>	920	8,642	8,467	1,095
<b>USSS</b>	568	1,120	811	877
<b>USCIS</b>	25,515**	144,559	144,748	25,326
<b>BTS</b>	0	0	0	0
<i>FLETC</i>	36	861	892	5
<i>CBP</i>	1,025***	3,283	3,886	422
<i>TSA</i>	193	1,123	522	794
<i>ICE</i>	235***	769	848	156
<i>FPS</i>	1	21	20	2
<b>TOTAL</b>	<b>28,743</b>	<b>161,117</b>	<b>160,902</b>	<b>28,958</b>

\* These entities did not exist prior to the creation of the Department of Homeland Security. FOIA requests for the Directorates were handled either by the Privacy Office or by component offices.

\*\* Formerly the Immigration and Naturalization Service.

\*\*\*Formerly the United States Customs Service.

**B. Disposition of Initial Requests**

<b>Directorate</b>	<b>Total Grants</b>	<b>Total Partial Grants</b>	<b>Total Denials</b>	<b>No Records</b>	<b>Referrals</b>	<b>Request Withdrawn</b>
<b>PO</b>	76	2	6	31	105	2
<b>OIG</b>	1	1	1	2	1	0
<b>S&amp;T</b>	0	0	0	0	0	0
<b>IAIP</b>	0	0	0	0	0	0
<b>EPR</b>	0	0	0	0	0	0
<i>FEMA</i>	157	78	39	44	24	38
<b>USCG</b>	5,762	500	69	585	762	215
<b>USSS</b>	33	178	31	197	0	5
<b>USCIS</b>	54,959	50,755	485	12,063	84	1,555
<b>BTS</b>	0	0	0	0	0	0
<i>FLETC</i>	825	45	2	11	0	7
<i>CBP</i>	1,473	622	294	756	227	88
<i>TSA</i>	55	97	61	68	40	46
<i>ICE</i>	46	445	18	118	142	14
<i>FPS</i>	16	3	1	0	0	0
<b>TOTAL</b>	<b>63,403</b>	<b>52,726</b>	<b>1,007</b>	<b>13,875</b>	<b>1,385</b>	<b>1,970</b>

## Disposition of Initial Requests (Continued)

Directorate	Records Not Reasonably Described	Not a Proper FOIA/PA Request	Not an Agency Record	Duplicate	Fee-Related Reason	Other*
PO	11	26	2	3	0	0
OIG	0	0	0	0	0	0
S&T	0	0	0	0	0	0
IAIP	0	0	0	0	0	0
EPR	0	0	0	0	0	0
FEMA	3	4	1	0	4	46
USCG	62	46	67	358	21	20
USSS	0	0	10	0	0	357
USCIS	9,453	205	1,520	9,457	924	3,288
BTS	0	0	0	0	0	0
FLETC	0	0	0	0	2	0
CBP	27	298	9	15	71	6
TSA	0	1	3	15	3	133
ICE	0	34	3	14	1	13
FPS	0	0	0	0	0	0
<b>TOTAL</b>	<b>9,556</b>	<b>614</b>	<b>1,615</b>	<b>9,862</b>	<b>1,026</b>	<b>3,863</b>

## \*Other Reasons For Nondisclosure

Component	Number of Times	Reason
FEMA	46	administratively closed after no response to still interested letter
USCG	20	available from other source
USSS	357	Failure to perfect request
USCIS	3,288	2,836 unable to locate; 452 old records
CBP	6	Administratively closed after response returned
TSA	133	3 litigation; 129 administratively closed after no response to still interested letter; 1 available from other source
ICE	13	Unable to locate requester

a. Number of times each FOIA exemption used

Directorate	(1)	(2)	(3)	(4)	(5)	(6)	(7)(A)	(7)(B)	(7)(C)
PO	0	0	0	0	0	4	0	0	2
OIG	0	10	0	0	0	0	0	0	1
S&T	0	0	0	0	0	0	0	0	0
IAIP	0	0	0	0	0	0	0	0	0
EPR	0	0	0	0	0	0	0	0	0
FEMA	1	6	2	45	27	56	0	0	1
USCG	24	24	25	74	154	375	87	0	93
USSS	2	102	17	1	27	42	3	0	168
USCIS	8	3,234	166	33	11,933	34,824	7,151	26	25,207
BTS	0	0	0	0	0	0	0	0	0
FLETC	0	1	0	9	17	24	1	0	17
CBP	1	359	0	157	162	88	16	3	403
TSA	3	9	118	18	13	31	3	0	26
ICE	5	447	3	20	26	70	32	0	468
FPS	0	0	0	1	1	2	0	0	0
<b>TOTAL</b>	<b>44</b>	<b>4,192</b>	<b>331</b>	<b>358</b>	<b>12,360</b>	<b>35,516</b>	<b>7,293</b>	<b>29</b>	<b>26,386</b>

Number of times each FOIA exemption used (Continued)

Directorate	(7)(D)	(7)(E)	(7)(F)	(8)	(9)
PO	0	0	0	0	0
OIG	0	0	0	0	0
S&T	0	0	0	0	0
IAIP	0	0	0	0	0
EPR	0	0	0	0	0
FEMA	0	0	0	0	0
USCG	20	9	4	0	0
USSS	34	78	5	0	0
USCIS	1,078	8,021	33	0	0
BTS	0	0	0	0	0
FLETC	0	0	0	0	0
CBP	27	162	2	0	0
TSA	0	0	2	0	0
ICE	63	200	2	0	0
FPS	0	0	0	0	0
<b>TOTAL</b>	<b>1,222</b>	<b>8,470</b>	<b>48</b>	<b>0</b>	<b>0</b>



VI. Appeals of Initial Denials of FOIA/PA Requests

Directorate	Number of Appeals Received in Fiscal Year 2003	Number of Appeals Processed in Fiscal Year 2003	Number of Appeals Completely Upheld In Fiscal Year 2003	Number of Appeals Partially Reversed In Fiscal Year 2003	Number of Appeals Completely Reversed in Fiscal Year 2003
PO	10	5	4	1	0
OIG	0	0	0	0	0
S&T	0	0	0	0	0
IAIP	0	0	0	0	0
EPR	0	0	0	0	0
FEMA	9	17	4	3	2
USCG	45	107	18	5	1
USSS	30	46	41	3	2
USCIS	940	140	1	0	0
BTS	0	0	0	0	0
FLETC	3	3	2	1	0
CBP	159	83	61	16	0
TSA	15	13	6	4	2
ICE*	0	0	0	0	0
FPS	0	0	0	0	0
<b>TOTAL</b>	<b>1,211</b>	<b>414</b>	<b>137</b>	<b>33</b>	<b>7</b>

a. Number of times each FOIA exemption was used in an appeal

Directorate	(1)	(2)	(3)	(4)	(5)	(6)	(7)(A)	(7)(B)	(7)(C)	(7)(D)	(7)(E)	(7)(F)	(8)	(9)
PO	0	0	0	0	0	2	0	0	0	0	0	0	0	0
OIG	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S&T	0	0	0	0	0	0	0	0	0	0	0	0	0	0
IAIP	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EPR	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FEMA	0	0	0	1	1	4	0	0	0	0	0	0	0	0
USCG	0	0	0	1	5	8	1	0	6	0	0	0	0	0
USSS	0	3	0	1	3	0	0	0	3	0	3	0	0	0
USCIS	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BTS	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FLETC	0	1	0	0	0	1	0	0	0	0	0	0	0	0
CBP	0	53	0	21	11	18	0	0	65	0	23	0	0	0
TSA	0	1	6	0	1	5	0	0	2	0	1	0	0	0
ICE*	0	0	0	0	0	0	0	0	0	0	0	0	0	0
FPS	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<b>TOTAL</b>	<b>0</b>	<b>58</b>	<b>6</b>	<b>24</b>	<b>21</b>	<b>38</b>	<b>1</b>	<b>0</b>	<b>76</b>	<b>0</b>	<b>27</b>	<b>0</b>	<b>0</b>	<b>0</b>

\* ICE appeals were handled by CBP; hence, their disposition is included in the figures reported for CBP

b. Other reasons for Non-Disclosure on Appeal

Directorate	No Records	Referrals	Withdrawn	Fee Related	Records Not Reasonably Described	Not a Proper FOIA Request	Not an Agency Record
<b>PO</b>	0	0	0	0	0	0	0
<b>OIG</b>	0	0	0	0	0	0	0
<b>S&amp;T</b>	0	0	0	0	0	0	0
<b>IAIP</b>	0	0	0	0	0	0	0
<b>EPR</b>	0	0	0	0	0	0	0
<i>FEMA</i>	1	0	0	2	0	0	0
<b>USCG</b>	0	0	66	0	0	0	0
<b>USSS</b>	0	0	0	0	0	0	0
<b>USCIS</b>	0	0	0	0	0	0	0
<b>BTS</b>	0	0	0	0	0	0	0
<i>FLETC</i>	0	0	0	0	0	0	0
<i>CBP</i>	3	0	1	0	0	1	0
<i>TSA</i>	0	0	0	0	0	0	0
<i>ICE*</i>	0	0	0	0	0	0	0
<i>FPS</i>	0	0	0	0	0	0	0
<b>TOTAL</b>	<b>4</b>	<b>0</b>	<b>67</b>	<b>2</b>	<b>0</b>	<b>1</b>	<b>0</b>

Other reasons for Non-Disclosure on Appeals (Continued)

Directorate	Duplicate Request	Other
<b>PO</b>	0	0
<b>OIG</b>	0	0
<b>S&amp;T</b>	0	0
<b>IAIP</b>	0	0
<b>EPR</b>	0	0
<i>FEMA</i>	0	5 Pending Litigation
<b>USCG</b>	0	17 Remanded for reprocessing
<b>USCIS</b>	0	139 Remanded for reprocessing
<b>BTS</b>	0	0
<i>FLETC</i>	0	
<i>CBP</i>	0	1 Glomar
<i>TSA</i>	0	1 Remanded for reprocessing
<i>ICE*</i>	0	0
<i>FPS</i>	0	0
<b>TOTAL</b>	<b>0</b>	<b>163</b>

\* ICE appeals were handled by CBP; hence, their disposition is included in the figures reported for CBP

**VII.** Compliance with time limits/status of pending requests

**A.** Median Time for Processing Requests

Directorate	Simple Requests		Complex Requests		Expedited Requests	
	Number of Requests Processed	Median Number of Days to Process	Number of Requests Processed	Median Number of Days to Process	Number of Requests Processed	Median Number of Days to Process
<b>PO*</b>	0	0	264	27	N/A	N/A
<b>OIG</b>	0	0	6	n/a	0	0
<b>S&amp;T</b>	0	0	0	0	0	0
<b>IAIP</b>	0	0	0	0	0	0
<b>EPR</b>	0	0	0	0	0	0
<i>FEMA*</i>	0	0	438	240	0	0
<b>USCG</b>	6,236	15	2,146	22	85	11
<b>USSS</b>	0	0	811	138	0	0
<b>USCIS</b>	110,305	15	34,343	39	100	10
<b>BTS</b>	0	0	0	0	0	0
<i>FLETC</i>	0	0	892	6	0	0
<i>CBP</i>	2,907	136	979	169	0	0
<i>TSA</i>	102	155	418	126	2	65
<i>ICE*</i>	0	0	848	189	0	0
<i>FPS</i>	0	0	20	14	0	0
<b>TOTAL</b>	<b>119,550</b>	<b>N/A</b>	<b>41,165</b>	<b>N/A</b>	<b>187</b>	<b>N/A</b>

\* These components did not use multi-track processing.

**B.** Status Of Pending Requests

Directorate	Number of Requests Pending at the End of Fiscal Year 2003	Median Number of Days Pending
<b>PO</b>	18	55.5
<b>OIG</b>	13	n/a
<b>S&amp;T</b>	0	0
<b>IAIP</b>	0	0
<b>EPR</b>	0	0
<i>FEMA</i>	250	373
<b>USCG</b>	1,095	22
<b>USSS</b>	877	133
<b>USCIS</b>	25,326	58
<b>BTS</b>	0	0
<i>FLETC</i>	5	4.5
<i>CBP</i>	422	305.1
<i>TSA</i>	794	126
<i>ICE</i>	156	96
<i>FPS</i>	2	30
<b>TOTAL</b>	<b>28,958</b>	<b>N/A</b>

**VIII. Comparisons with Previous Years**

This is the first year as the Department of Homeland Security. Due to this fact the Department will use Fiscal Year 2003 as its baseline year. This will give the Department data for comparison in Fiscal year 2004.

During this year, DHS received 194 requests for expedited treatment, and granted 187 of them.

**IX. Costs/FOIA/PA Staffing**

Directorate	Staffing Levels			Total Costs (Staff and Resources combined)		
	Number of Full-time Personnel	Number of Personnel with Part-time FOIA/PA Duties (In Total Work-years)	Total Number of Personnel (In Work-years)	FOIA Processing (Including Appeals)	Litigation-related Activities	Total Costs
<b>PO</b>	1	2.5	3.5	\$312,500	0	\$312,500
OIG	1.5	0	1.5	\$112,586	0	\$112,586
<b>S&amp;T</b>	0	0	0	0	0	0
<b>IAIP</b>	0	0	0	0	0	0
<b>EPR</b>	0	0	0	0	0	0
<i>FEMA</i>	2	2.75	4.75	\$276,278	\$6,000	\$282,278
<b>USCG</b>	15	27.91	42.91	\$698,464	\$8,000	\$706,464
<b>USSS</b>	13	1.72	14.72	\$1,201,644	\$60,000	\$1,261,644
<b>USCIS</b>	246	0	246	\$14,604,393	\$82,116	\$14,686,509
<b>BTS</b>	0	0	0	0	0	0
<i>FLETC</i>	1	1	2	\$164,009	\$0.00	\$164,009
<i>CBP</i>	14	23	37	\$1,155,509	\$122,135	\$1,277,644
<i>TSA</i>	10	3	13	\$912,226	\$52,540	\$964,766
<i>ICE</i>	17	15	32	\$1,393,451	\$80,000	\$1,473,451
<i>FPS</i>	13	0	13	\$683,000	0	\$683,000
<b>TOTAL</b>	<b>333.5</b>	<b>76.88</b>	<b>410.38</b>	<b>\$21,514,060</b>	<b>\$410,791</b>	<b>\$21,924,851</b>

**X. FOIA Fees**

A. Total Fees Collected:	<b>\$270,384.31</b>
B. Percentage of Total Costs:	<b>1.02%</b>

**XI. Department of Homeland Security FOIA Implementing Regulations**

The Department of Homeland Security FOIA Implementing Regulations can be found at 68 Fed. Reg. 4056 (January 27, 2003) and at: [http://www.dhs.gov/interweb/assetlibrary/FOIA\\_FedReg\\_Notice.pdf](http://www.dhs.gov/interweb/assetlibrary/FOIA_FedReg_Notice.pdf).



# **U.S. Department of Homeland Security Privacy Office OUTREACH HIGHLIGHTS**

*(2003 – 2004)*

- Chicago – Guest speaker at Privacy Conference 2003  
“Information, Security and Ethics in the Digital Age”
- Washington, D.C. – DHS/Information Analysis and Infrastructure Protection Conference:  
Homeland Security and the Private Sector, Washington, DC  
“Balancing the Need for Security with Economic Prosperity”
- Washington, D.C. – NSTC Biometrics Social/Legal Privacy Subgroup
- Washington, D.C. – Markle Event
- Washington, D.C. – Air Transport Association Conference  
Briefing to senior advisory committee
- New York City, NY – State Bar Association Annual Meeting – Guest Speaker  
“Balancing Privacy and Security in a Post 9-11 World”  
and presentation to the International Law and Practice Section
- Washington, D.C. – House Subcommittee on Commercial and Administrative Law  
Legislative Oversight Hearing
- Washington, D.C. – Georgetown University Law Center – Guest Speaker  
“Privacy & Government Record Systems”
- Washington, D.C. - International Association of Privacy Professionals Privacy and Data Security  
Summit & Expo – Guest Speaker  
“Protecting Privacy in an Insecure World”
- Washington, D.C. - Center for Strategic and International Studies  
Roundtable on Radio Frequency Identification – Guest Speaker
- Washington, D.C. – DHS/Science and Technology Event via conference call
- Arlington, VA – DHS/Transportation Security Administration – Privacy Education Week – Speaker

- Washington, D.C. – Secretary Ridge Council for Excellence in Government initiative – team member for establishing the privacy and FOIA focus for the council’s Town Hall meetings to be held throughout middle America
- Washington, D.C. – Chamber of Commerce Homeland Security Task Force – To discuss privacy and security issues, a view of key programs impacting security
- Arlington, VA – Search Conference – Symposium on Integrated Justice Information Systems – plenary session Keynote Address, and panelist  
“Privacy’s Prospects in the Information Age”
- Washington, D. C. – American Bar Association
  - Infrastructure Security Panel – conference call
  - Spring Meeting – panelist – CII and Infrastructure Security
  - Conference on “Counterterrorism, Technology and Privacy”
- Washington, D.C. – CDT
  - Workshop on Privacy Impact Assessments
  - Workshop on FISMA
- Washington, D.C. – Virginia Tech Conference – Keynote Address  
“Fostering Public Private Partnerships for Security and Privacy,”
- Washington, D.C. – Council for Excellence in Government  
Privacy and security working group meeting
- Washington, D.C. – Brookings Institution Roundtable – To discuss cooperative efforts between the media and high profile government personnel
- Vienna, VA – Information Technology Association of America Homeland Security Committee  
guest speaker on critical privacy issues and their effect on IT deployment
- Washington, D.C. – U.S. Department of Health and Human Services Data Council Privacy Committee  
Keynote Address – privacy issues impacting their various programs
- Austin, Texas – American Legislative Exchange Council – Guest Speaker  
“Securing the Homeland While Preserving Privacy”
- Washington, D.C. – Electronic Privacy Information Center 10<sup>th</sup> Anniversary – Keynote Address  
“Privacy Protection & Technology Post 9/11”
- Washington, D.C. – Supercomputer Center Workshop: “Workshop on Privacy Technology for Sharing Justice Data” Contributed policy paper regarding the challenge of distributed data sharing and a policy paper on the related privacy framework
- Chicago, IL – Conference on Counterterrorism and Privacy
- Washington, D.C. – Public Workshop – Radio Frequency Identification – Guest Speaker  
“Applications and Implications for Consumers”
- Washington, D.C. – Enhanced International Travel Security Initiative – Guest Speaker  
“Privacy & Policy Issues”

- Washington, D.C. – MIT Media Lab Workshop – Guest Speaker  
“Modern Technologies and Applications for Homeland Security”
- Washington, D.C. – International Visitor Program through Department of State, Office of International Visitors, Bureau of Educational and Cultural Affairs – Guest Speaker  
“The DHS Privacy Office and privacy issues related to biometrics”
- Baltimore, MD – The 2004 DHS Security Conference and Workshop
- Brussels and Dublin – Initiated discussions with European Union Committee members relative to the prominent international data privacy concerns
- Berlin, Germany – Met with key interagency and ministry data protection officials, legal advisors and party officials in support of ongoing privacy related issues
- Brussels, Belgium – Addressed Parliament on their key data protection issues, specifically passenger name record concerns, and met with numerous Belgian data privacy authorities, including economic advisors, academics and government officials
- Rome, Italy – Met with key officials of the Ministries for Justice, Commerce, Technology and Communications, as well as Data Commission authorities
- Vienna, Austria – Joined various Austrian data privacy experts and economic and legal advisors to carry on discussions associated with PNR data protection and other relevant issues
- Paris, France – Visited with prominent data protection authorities in the European Union Commission to address pertinent data privacy concerns
- Sydney, Australia – International Data Protection and Privacy Professionals Conference - keynote speaker
- Brussels – EU Commission  
Biometric identifiers in international travel documents and the effect of biometrics on key international systems and programs
- Washington, D.C. – Cyber security with Director General for Commerce and Information Policy
- Poland – Ministry of International Affairs  
To encourage data sharing and open discussion on policy, programs, and systems –  
Focus: data security and information technology
- Spain – Data Protection Agency  
Discussion of programs and systems of interest; policy and an update on the current activities within the Privacy Office
- Brussels – Guest Speaker and Observer at a meeting of Europol’s Joint Supervisory Body (on data protection in law enforcement)
- Brussels – Attended EU Parliament’s Civil Liberties Committee on privacy impact of Customs and Board Protection and Transportation Security Administration’s use of passenger name record data. Engaged EU privacy representatives in discussion of PNR policy proposals.

- Berlin – Participated in an international meeting on privacy notices with data protection commissioners, privacy and consumer advocates, and multinational business representatives.
- Paris – Meeting of the Organization for Economic Cooperation and Development (OECD) to discuss enhanced international travel security, biometrics and the working party's general privacy agenda.
- Buenos Aires – Participated in established meetings of the International Working Party on Data Protection in Telecommunications, participated in an outreach event with Privacy Advocates hosted by the Public Voice. Attended a 2-day meeting on consumer protection issues hosted by the U.S. Federal Trade Commission.
- Washington, D.C. – Hosted international data privacy commissioners to discuss programs and systems of interest, policy and an update on the current activities within the Privacy Office
  - Data Commissioner – Hong Kong
  - Commissioner of Information and Privacy, Ontario, Canada
  - Federal Privacy Commissioner of Canada
  - Information Commissioner, Data Protection Agency-United Kingdom
- Washington, D.C. – Hosted these individuals at the request of the State Department to discuss educational programming
  - Journalist - Republic of Karzakhstan
  - Editor, Journalist, Educator - Republic of Karzakhstan
- Washington, D.C. – Guests of the Privacy Office through arrangements made by the Department of State and Meridian (as part of the International Visitors Program) for discussions relating to the use of biometric identifiers in travel documents and related data privacy issues:
  - Director, Passport Affairs, Austria
  - Attache, Ministry of Foreign Affairs, Denmark
  - Project Manager, VIS and EU Comm, Belgium
  - Project Manager, Ministry of Foreign Affairs, Finland
  - Deputy Director, Ministry of Foreign Affairs, Lithuania
  - Ministry of Justice, Netherlands
  - Inspector, Dept of Counterfeit Documentation, Spain
  - Deputy Head, Terrorism and Protection Unit, United Kingdom
  - Assistant Director, Immigration Service, United Kingdom
- Washington, D.C. – Hosted Commissioner of Information and Privacy, Ontario, Canada
- Washington, D.C. – Hosted member of the Australian National Computer Emergency Response Team and Former Federal Privacy Commissioner, Australia